VŠB TECHNICKÁ UNIVERZITA OSTRAVA
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

MDM systémy pro vzdálenou správu Android zařízení

MDM Systems for Remote Management of Android Devices

Marcel Grygar

Bakalářská práce

Vedoucí práce: Ing. Lukáš Kapičák

Ostrava, 2021

Abstrakt

Bakalářská práce je zaměřená na vzdálenou správu mobilních zařízení s operačním systémem Android ve firemním prostředí. Cílem práce je představení různých řešení pro mobilní telefony, výběru vhodného řešení, instalace a konfigurace a následně testování řešení na pěti různých Android zařízeních.

Teoretická část se zaměřuje na uplatnění Mobile Device Manager ve firemním prostředí a následně na možnosti open source a placených řešení, které existují pro operační systém android.

Praktická část práce se věnuje instalaci a konfiguraci vybraného MDM řešení a jeho otestování na pěti různých android zařízeních.

Klíčová slova

Správa mobilních zařízení; Správa podnikové mobility; Sjednocená správa koncových bodů; Správa android zařízení; IBM MaaS360 with Watson; Samsung Knox Manage; Headwind MDM; ManageEngine MDM; Android; Android Enterprise;

Abstract

Bachelor thesis is focused on remote mobile of device management with the Android operating system in a corporate environment. The aim of the work is to present various solutions for mobile phones, select a suitable solution, install and configure then test it on five different Android devices.

The theoretical part is focuses on the application of Mobile Device Management in the corporate environment and then on the possibilities of Open-source software and paid solutions that exist for the Android operating system.

The practital part of the work is devoted to the installation and configuration of a selected MDM solution and test it on five different Android devices.

Keywords

Mobile Device Management; Enterprise Mobility Management; Unified Endpoint Management; Android device management; IBM MaaS360 with Watson; Samsung Knox Manage; Headwind MDM; ManageEngine MDM; Android; Android Enterprise;

Poděkování

Rád bych na tomto místě poděkoval svému vedoucímu práce Ing. Lukášovi Kapičákovi za připomínky, odborné rady, doporučení a poskytnutá zařízení. Také bych chtěl hlavně poděkovat své přítelkyni za korekturu textu.

Mé poděkování patří také doc. Mgr. Jiřímu Dvorskému, Ph.D. za konzultace a technické rady k technologii LateX.

Obsah

Seznam použitých zkratek a symbolů

MDM	–	Mobile Device Management
EMM	–	Enterprise Mobility Management
UEM	–	Unified Endpoint Management
COPE	–	Corporate Owned Personal Enable
COBE	–	Corporate Owned Business Only
BYOD	–	Bring Your OwnDevice
CYOD	–	Choose Your Own Device
MAM	–	Mobile Application Management
MCM	–	Mobile Content Management
MSM	–	Mobile Security Management
VPN	–	Virtual Private Network
LTE	–	Long Term Evolution
GSM	–	Global System for Mobile Communication
NFC	–	Near Field Communication
OTA	–	Over The Air
WLAN	–	Wireless Local Area Network
UMTS	–	Universal Mobile Telecommunications Standard
API	–	Application Programming Interface
OHA	–	Open Handset Alliance
MTD	–	Mobile Threat Defense
SIEM	–	Security Information and Event Management
IDaaS	–	Identity as a Service
GMS	–	Google Mobile Services
SMS	–	Short message service
APK	–	Android application package
HTTP	–	Hypertext Transfer Protocol
HTTPS	–	Hypertext Transfer Protocol Secure
FQDN	–	Fully Qualified Domain Name

ART	–	Android Runtime
ISP	–	Internet service provider
WAN	–	Wide Area Network

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Za minulou dekádu se struktura mobilních zařízení ve firemním prostředí razantně změnila. Mobilní zařízení začínají být nedílnou součástí firemního prostředí. Zaměstnavatel se snaží zvýšit efektivitu a spokojenost svých zaměstnanců tím, že jim umožňuje pracovat mimo kancelář. S narůstajícím počtem mobilních zařízení vzniká potřeba tyto mobilní zařízení spravovat a kontrolovat.

Téma této bakalářské práce je aktuální, jelikož se většina firem přesunula na práci z domu. Podle průzkumu [1] v roce 2021 chytré telefony v pokročilejších zemích vlastní v průměru 73,5 % populace. Ve firemním prostředí se tento trend promítl také a je třeba na něj reagovat. S rostoucím počtem mobilních zařízení, firemních dokumentů a dat ve firemním prostředí je téměř nutno tyto data a zařízení kontrolovat. Prostřednictvím Mobile Device Managementu jsme schopní nastavit politiku a bezpečnostní pravidla pro tyto mobilní zařízení. Dále je možnost využít Mobile Device Management pro vzdálené vymazání dat, nastavování různých politik pro různé skupiny a různé uživatele. Nespornou výhodou tohoto řešení je hromadná vzdálená správa, tedy není nutno, aby každé zařízení prošlo IT oddělením a tím šetří jak čas, tak náklady, které exponenciálně rostou s každým novým zařízením ve firemním prostředí.

Cílem práce je představit nástroje pro správu mobilních zařízení a ukázat jejich možnosti. Konkrétně se bakalářská práce zabývá operačním systémem Android a může posloužit jako návod pro správu mobilních zařízení ve firemním prostředí.

Teoretická část se věnuje popisu správy mobilních zařízení. Kapitola 2 popisuje, co si představujeme pod pojmem mobilní zařízení, jak funguje správa na mobilních zařízeních, a jaké jsou její hlavní funkce. Další část představuje, jaké jsou výhody a nevýhody správy mobilních zařízení z pohledu zaměstnavatele. Kapitola 2.3 obsahuje různé typy zařízení, které ve firemním prostředí existují. Důležitou kapitolou je představení rozdílných přístupů pro správu mobilních zařízení, rozdílů mezi těmito přístupy a jejich historie. Nejdůležitější částí je popis šesti vybraných softwarů pro správu zařízení. Kapitola 3 představí výběr vhodného řešení pro operační systém Android. Součástí této kapitoly je popis, jak funguje správa zařízení na této platformě, jak vypadá architektura, a jak si Android dokáže poradit se správou zařízení na své platformě.

Praktická část bakalářské práce představí možnosti čtyř vybraných softwarových nástrojů. V této části je popis administrátorského rozhraní, a návod jak mobilní zařízení přidat do správy mobilních zařízení, včetně nastavení serveru pro správu. Následně se řešení otestuje na vybraných Android zařízeních.

Kapitola 2

Mobile Device Management

Mobile Device Management (dále jen MDM) je softwarové řešení pro většinu mobilních zařízení ve firemním prostředí. Pod mobilním zařízením si můžeme představit jakýkoliv přenosný přístroj, který má vlastní napájení. Obvykle je vybaven displejem. Mobilní zařízení, která se objevují v práci, budou hlavně zařízení, která komunikují skrze technologii WiFi nebo přes mobilní datovou síť a mají mobilní operační systém. Tyto mobilní operační systémy běžně umožňují instalaci a spuštění aplikací třetích stran. Další charakteristikou mobilních zařízení, které jsou součástí práce, je možnost odpojení od napájecí sítě a možnost nadále tato zařízení využívat. MDM si klade za cíl zajistit maximální bezpečnost a funkčnost mobilního zařízení ve firemním prostředí. MDM tedy slouží pro vzdálenou správu mobilních zařízení, umožňuje konfiguraci těchto zařízení, tak aby odpovídala nastaveným zásadám a požadavkům ve firmě.

MDM se obvykle implementuje s použitím aplikací třetích stran, které mají možnost spravovat různé zařízení od různých dodavatelů mobilních zařízení. Jak bylo zmíněno různé mobilní zařízení jsou od různých dodavatelů a také mají jiný operační systém, přestože se práce zabývá pouze operačním systémem Android, je potřeba zmínit, že různé řešení jsou kompatibilní na různých operačních systémech (Citrix Endpoint Managment podporuje správu zařízení na Windows, iOS, Android nebo MacOS) nebo jsou vyvíjeny na jeden operační systém (Jamf Now podporuje čistě iOS). Ještě před pár lety nebylo možné mít pod jedním řešením celé firemní prostředí, včetně mobilních zařízení a stolních počítačů.

Hlavní funkcí MDM je zvýšení zabezpečení, podpory zařízení a firemních funkcí s co největším zachováním zaměstnanecké flexibility. Spousta firem využívá správu mobilních zařízení, aby mohla zařízení monitorovat a sledovat (například polohu, aktivitu a stav zařízení). Mezi další funkce MDM patří aktualizace zařízení, funkcí aplikací a možnost efektivně diagnostikovat zařízení a odstraňovat problémy na dálku. Další z funkcí je zajištění, aby zaměstnanec využíval zařízení konzistentně a podporovatelným způsobem.

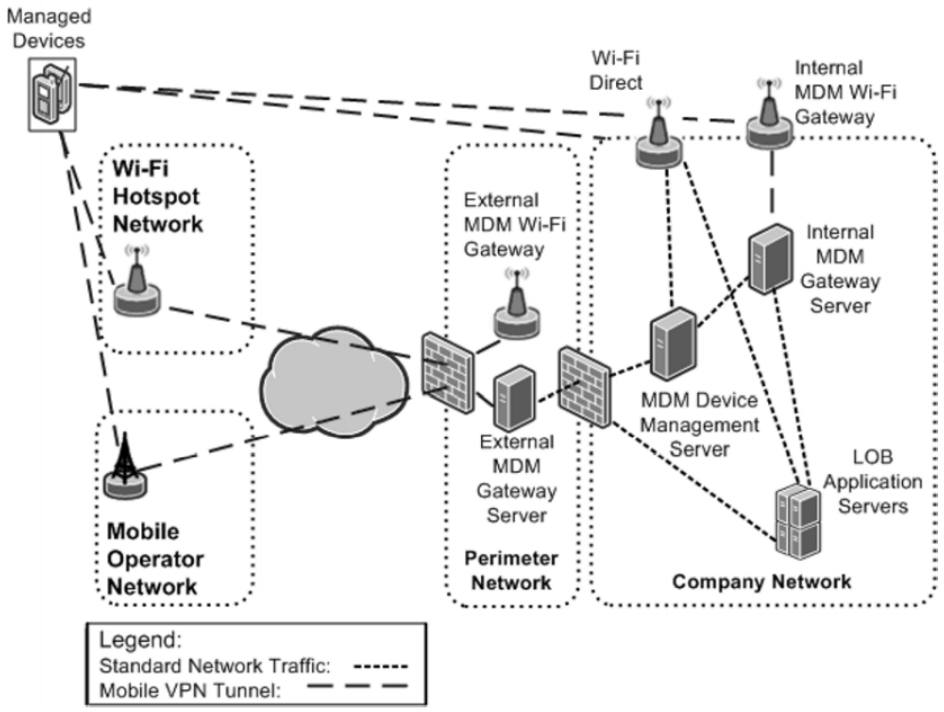
MDM řešení obvykle zahrnuje serverovou a klientskou část. Serverová část odesílá příkazy pro správu do mobilního zařízení. Klientská část běží na spravovaném zařízení a přijímá a implementuje

příkazy pro správu. V některých případech MDM řešení dodává prodejce server i klienta, zatímco někteří prodejci dodávají klienta a server skrze dodavatele.

Přidání mobilního zařízení do MDM se obvykle provádí přes bezdrátovou komunikaci a je zde také možnost přidat zařízení přes fyzické rozhraní. U bezdrátové komunikace se můžeme setkat s pojem Over the Air.

Over the air (OTA) je synonymum pro bezdrátovou komunikaci, označuje standard pro nastavení mobilního zařízení a jeho konfiguraci, která se provádí zcela bez jakéhokoliv fyzického spojení mezi mobilním zařízením a serverem pro správu mobilního zařízení. K jakémukoliv přenosu dat dochází prostřednictvím bezdrátových sítí jako je NFC (Near Field Communication), bezdrátová místní síť WLAN (Wireless Local Area Network), Bluetooth nebo standardy mobilní komunikace jako jsou GSM (Global System for Mobile Communication), UMTS (Universal Mobile Telecommunication System) nebo LTE (Long Term Evolution).

Tato bezdrátová komunikace má jednoduché a pohodlné ovládání, monitorování a údržbu mobilních zařízení bezdrátově, ale zároveň má omezení a bezpečnostní rizika. Prosazovat bezpečnostní zásady jako zamknutí, vymazaní telefonu, shromažďovaní údajů a dat je snadno uskutečnitelné. Na druhou stranu není možné zálohovat nebo aktualizovat, pokud provádíme bezpečnostní zásady. Proto je zaměstnanec odpovědný, za to aby zařízení aktualizoval a zálohoval. Přenos dat přes bezdrátovou síť navíc nelze kontrolovat, a proto musí být šifrován nebo zabezpečen pomocí virtuální privátní sítě (VPN), viz obrázek 2.1.



Obrázek 2.1: Zabezpečená bezdrátová komunikace (Asgar, 2013) [2]

Způsob implementace MDM serveru se dělí na dva typy. Jeden z typů je tzv. on-premise neboli in-house a druhý z typů je tzv. hosted neboli cloud based. Firma by měla učinit rozhodnutí, jestli využije řešení založené na cloudu (Hosted/ cloud based) nebo místní řešení (on-premise/ in-house). Místní řešení poskytuje maximální flexibilitu, pokud jde o připojení k místní IT infrastruktuře. Počáteční investice místní řešení je dražší, oproti řešení založená na cloudu, jelikož musí zaměstnavatel v rámci určitého řešení vyškolit zaměstnance v údržbě MDM serveru, instalaci aplikací třetích stran pro kontejnerizaci, firemní obchod s aplikacemi nebo bezpečnostní aktualizaci. Měsíční částka u místního řešení je oproti cloudovému řešení nižší. Software as a Service (SaaS) je služba, kterou dnes nabízí většina prodejců MDM. Server MDM je hostován prodejcem a poskytuje potřebné aplikace ihned pro optimální provoz MDM. Zejména pro malé a střední podniky je takový scénář výhodnější z důvodu výše zmíněných vysokých nákladů na vstup a údržbu místního řešení.

2.1 Výhody MDM řešení ve firemním prostředí z pohledu zaměstnavatele

- Soukromé zařízení ve firemním prostředí.
  - Flexibilita a zvýšena produktivita zaměstnance.
  - Levnější náklady pro zaměstnavatele, tím že se zbavuje nákladu na pořizování mobilního zařízení.
- Snadná vzdálená správa a jednoduchost.
  - Hromadné aktualizace všech zařízení, které jsou pod správou MDM.
  - Díky možnostem automatizace značně snižuje zátěž na IT pracovníky.
  - Automatická registrace zařízení. Existuje sada programů, která umožňuje automatický zápis, díky tomuto procesu lze registrace zařízení urychlit. Jakmile zaměstnanec obdrží zařízení a zapne jej, zařízení automaticky použije všechna nastavení a konfigurace poskytované podnikem. Tímto také zajistíte, že MDM bude na zařízení povinné.
- Bezpečnost.
  - Prevence úniku citlivých dat při krádeži telefonu. Možnost smazat vzdáleně firemní data.
  - Zabezpečení firemní sítě, například deaktivování nebezpečného zařízení.
  - Automatická záloha dat. V případě ztráty nebo poškození zařízení, nedojde k ztrátě dat.
  - Kontrola stahování aplikací do mobilu, které by mohly zapříčinit únik dat.
  - Prosazování bezpečnostní politiky.

2.2 Nevýhody MDM řešení ve firemním prostředí z pohledu zaměstnavatele

- Mezery v bezpečnosti.
  - Z psychologického hlediska si uživatel může myslet, že je jeho zařízení zabezpečené a může tedy opomenout fakt, že nechal odemknuté zařízení bez dohledu. MDM řešení nemůže zabránit všem bezpečnostním rizikům.
  - MDM zařízení nemůže zabránit únikům dat z cloudových služeb.
- Práce s daty.
  - Pomocí MDM není možné hlídat a sledovat data v rámci aplikace nebo jejího procesu.
- Pravidelná bezpečnostní kontrola.
  - Firma by samotné MDM řešení měla kontrolovat pomocí bezpečnostních auditů.
- Soukromé zařízení ve firemním prostředí.
  - Zaměstnanec může odmítnout politiku MDM na svém soukromém zařízení, kvůli zhoršení komfortu nebo podezření, že by mohl být zaměstnavatelem špehován. Více o tomto tématu v kapitole 2.3.
  - Jakékoliv mobilní zařízení, které je využito ve firemním prostředí jako soukromé, představuje bezpečnostní riziko. Únik dat přes mobilní aplikace, které se využívají na mobilním zařízení.

2.3 Typy zařízení ve firemním prostředí

Zaměstnanci firmy mohou využívat v práci své mobilní zařízení pro pracovní účely. Pokud začnou své soukromé zařízení využívat pro práci, tak se používá označení Bring Your Own Device (dále jen BYOD). Zaměstnanci většinou chtějí skloubit soukromý život s prací a využívají svoje mobilní zařízení pro pracovní účely, například pro emailovou komunikaci přes firemní síť. Zranitelnost těchto zařízení je vysoká. To také dokazuje průzkum od americké společnosti NowSecure, která se zabývá bezpečností v oblasti mobilních technologií. Cílem průzkumu bylo otestovat 250 oblíbených aplikací. Na závěr bylo zjištěno, že 70% aplikací mělo únik citlivých dat, je tedy na místě BYOD zařízení dostatečně zabezpečit, aby mohla využívat firemní síť a nedošlo k úniku citlivých firemních dat. [3]

Problém při použití osobních zařízení pro pracovní účely je ten, že zaměstnavatel musí počítat s ochranou osobních údajů vlastních zaměstnanců. Toto musí být zohledněno v pracovní smlouvě, kde tyto náležitosti musí být právně ošetřeny. Zaměstnanec by si měl uvědomit, že mu zaměstnavatel může kdykoliv osobní data v zařízení přes MDM řešení kompletně vymazat. Další nevýhoda pro zaměstnance je možnost sledování zařízení, sledování nainstalovaných aplikací a zakázání různých

aplikací. Nevýhody jako je zakázání různých aplikací nebo sledování nainstalovaných aplikací se dají vyřešit oddělením osobního prostoru a pracovního prostoru pomocí kontejnerů. Tyto kontejnery dokážou omezit použití pracovního prostoru mimo lokalitu nebo firemní síť. Výhoda pro zaměstnance, který je nucen mít mobilní zařízení pod MDM je, že nemusí mít dvě mobilní zařízení, zařízení je pro něho známé a nemusí se přizpůsobovat novému zařízení.

Také by se nemělo zapomínat, že samotné zařízení, které vlastní zaměstnanci a bude spadat pod BYOD, by mělo podléhat také bezpečnostnímu auditu, aby mohla být implementováno do firemního prostředí. Výběr jakéhokoliv mobilního zařízení s odlišnými operačními systémy by mohlo způsobit bezpečnostní rizika a zvýšení nákladů na správu a bezpečnost. Samotné verze operačních systémů jsou diametrálně odlišené, obzvlášť u mobilního operačního systému Android. Spousta firem tedy nedovolila svým zaměstnancům použití osobních mobilních zařízení pro pracovní účely.

Dalším typem zařízení je Corporate Owned Personal Enabled (dále jen COPE). Tento typ zařízení nakupuje firma pro zaměstnance. Zaměstnanec má firemní zařízení, které může využívat také pro osobní účely. Pro firmu je počáteční investice vyšší, než u zařízení BYOD. Na druhou stranu, správným výběrem mobilního zařízení můžeme snížit navýšení nákladu na správu a bezpečnost. Mobilní zařízení jsou zaměstnancům známé a je pro ně tedy jednodušší a pohodlnější je využívat pro pracovní účely, tím pádem se zvyšuje zaměstnanecká produktivita a efektivita. Jedna z nevýhod pro zaměstnance je fakt, že můžou být jejich data z mobilního zařízení vymazána bez jakékoliv dohody, zatímco u BYOD zařízení musí mít zaměstnavatel od zaměstnance písemné svolení například v rámci smlouvy. U zařízeních MDM, které podporují oddělení pracovního a soukromého prostoru, nehrozí smazání soukromého prostoru, jelikož při příkazu smazání z konzole MDM se smaže pouze pracovní prostor.

Nejbezpečnějším typem zařízení je Corporate Owned Business Only (dále jen COBO). V tomto případě zaměstnanec dostává od firmy zařízení, které může využít pouze pro pracovní účely. Kvůli citlivým informacím je přísně zakázáno použití pro soukromé účely.

Posledním typem zařízení je Choose Your Own Device (dále jen CYOD). Zaměstnanec si vybírá z před připraveného listu mobilních zařízení. Firma sestaví seznam schválených zařízení, která splňují kritéria firmy a zaměstnance. Firmy také můžou dopředu nainstalovat aplikace na zařízení. Tyto zařízení zaměstnanec může využít také pro osobní účely.

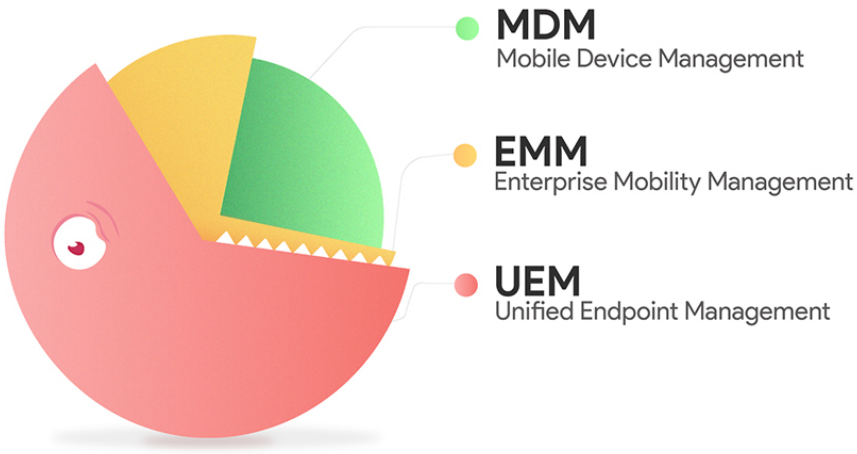
Ve firmách, kde jsou uložená citlivá data, je vhodné zvolit COBO. Pokud firma nechce investovat peníze do mobilních zařízení pro zaměstnance, je vhodné zvolit BYOD. BYOD dává zaměstnancům větší svobodu na úkor většího rizika úniku dat. COPE se využívá zřídka, kvůli vysokým investičním nákladům, možností vymazání dat a obavy zaměstnance ohledně ochrany jeho soukromí. CYOD je zajímavé řešení, jelikož dává na výběr z několika mobilních zařízení, které firma vybrala. CYOD je dost podobné BYOD, akorát nabízí větší bezpečnostní výhody oproti BYOD zařízením, a také je snažší je spravovat a podporovat ve srovnání s BYOD řešením. Je nutné seznam zařízení udržovat a schvalovat nové zařízení.

2.3.1 Samsung Knox

Samsung Knox je bezpečnostní implementace od společnosti Samsung, která je předinstalovaná na vybraných Android zařízeních společnosti Samsung a je zabudovaná do hardwaru i softwaru nejnovějších zařízení Samsung. Není to tedy přímo označení pro typ zařízení, ale doplňuje BYOD, CYOD a COPE. Samsung Knox zachází s pracovním prostorem zařízení odděleně od vašeho osobního prostoru pro Android. Tím je zajištěno, že nikdo jiný než samotný uživatel nebude mít přístup k části vašeho telefonu Samsung, která obsahuje aplikace pro běžné a osobní použití. Zároveň zachází s pracovním prostorem telefonu způsobem, který vyžaduje dodržování zásad společnosti. Pokud budeme hledat MDM řešení pro zařízení od společnosti Samsung, bylo by vhodné vybrat takové řešení, které umí pracovat se Samsung Knox. Samsung Knox dokáže oddělit a izolovat osobní a firemní uživatelská data. Samsung Knox patří mezi nejbezpečnější zabezpečení co se mobilních zařízení týče, používají ho jak velké korporace, tak vlády. Seznam zařízení, které mají implementované Samsung Knox, je k nalezení zde [4].

2.4 Rozdílné nástroje pro správu mobilních zařízení

Pokud budeme hledat řešení MDM, tak se setkáme s názvy jako jsou Enterprise Mobility Management (dále jen EMM) nebo Unified Endpoint Management (dále jen UEM), viz obrázek 2.2. Často se stává, že se tyto názvy pletou a v praxi se zaměňuje jejich význam. Znalost rozdílů je důležitá, aby se do firemního prostředí nenasazovala řešení, která mohou být finančně nákladné. Menší společnosti nemusí hned nakupovat komplexní řešení, jako je UEM a můžou zůstat u MDM nebo EMM.



Obrázek 2.2: Nástroje pro správu, převzato z [5]

Samotné MDM má problém v tom, že nedokáže tak efektivně pracovat s daty. Nedokáže mít úplnou kontrolu nad aplikacemi třetích stran a firemními dokumenty.

EMM se tedy skládá z pěti důležitých částí:

- MDM (Mobile Device Management) – správa mobilního zařízení ve firemním prostředí,
- MAM (Mobile Application Management) – správa aplikací nainstalovaných na mobilním zařízení,
- MCM (Mobile Content Management) – správa dokumentu na mobilním zařízení,
- MSM (Mobile Security Management) – zabezpečení dat na mobilním zařízení a
- MAM (Mobile Asset Management) – správa aktiv na mobilním zařízení.

2.4.1 Mobile Asset Management

Mobile Asset Management je součástí Mobile Device Management. Mobile Asset Management popisuje přístup pro správu ovládání, monitorování a optimalizaci mobilních zařízení. Záměrem Mobile Asset Management je získat přesné množství dat ke kontrole a monitorování mobilních zařízení v prostředí společností a vytvořit databázi registrovaných mobilních zařízení a jejich uživatelů. Hlavní účel Mobile Asset Management je tedy registrace zařízení, monitorování, kontrolování a udržování mobilního zařízení, a také následné vyřazení z provozu. Podrobněji se o tomto tématu píše zde [2].

2.4.2 Mobile Application Management

S přílivem BYOD, CYOD a COPE zařízení, se samotné MDM řešení nedokázalo vypořádat s osobními daty na firemním zařízení. Zde tedy přichází Mobile Application Management (MAM). Mobile Application Management dokáže oddělit firemní aplikace a data od osobních dat a aplikací pomocí kontejnerizace. Mobile Application Management je část, která se zaměřuje na zajišťování, řízení a údržbu mobilních aplikací na mobilních zařízeních. Hlavním účelem Mobile Application Management je automaticky poskytovat veřejné a interně vyvinuté aplikace koncovým uživatelům. Kromě toho lze dosáhnout zajišťování předdefinovaných aplikací a řízení jejich používání. Je také možné založit podnikový obchod s konkretními aplikacemi pro zaměstnance, které lze distribuovat, ovládat a udržovat. Mobile Application Management a Mobile Asset Management se navzájem doplňují. Zatímco Mobile Asset Management zajišťuje vysokou míru kontroly nad mobilními zařízeními a základním hardwarem, Mobile Application Management poskytuje vysoký stupeň kontroly nad mobilními aplikacemi, od jednoduchého zabalení aplikace, až po aplikace zabezpečeného kontejneru. Výše uvedené funkce umožňují řídit a monitorovat používání mobilních aplikací a definovat odpovídající úroveň zabezpečení na aplikační vrstvě. Podrobnější informace k tomuto tématu jsou dostupné v této literatuře [2].

2.4.3 Mobile Content Management

Mobile Content Management (dále jen MCM) je sada technologií, která se zaměřuje na zajišťování, řízení a monitorování zabezpečeného přístupu k podnikovým datům a přenosu dat na mobilních zařízeních a koncových bodech. Hlavním účelem správy mobilního obsahu je poskytovat a sdílet soubory mezi různými síťovými připojeními. Může to být sdílení souborů v místní síti organizace nebo v úložišti dat pro mobilní klienty.

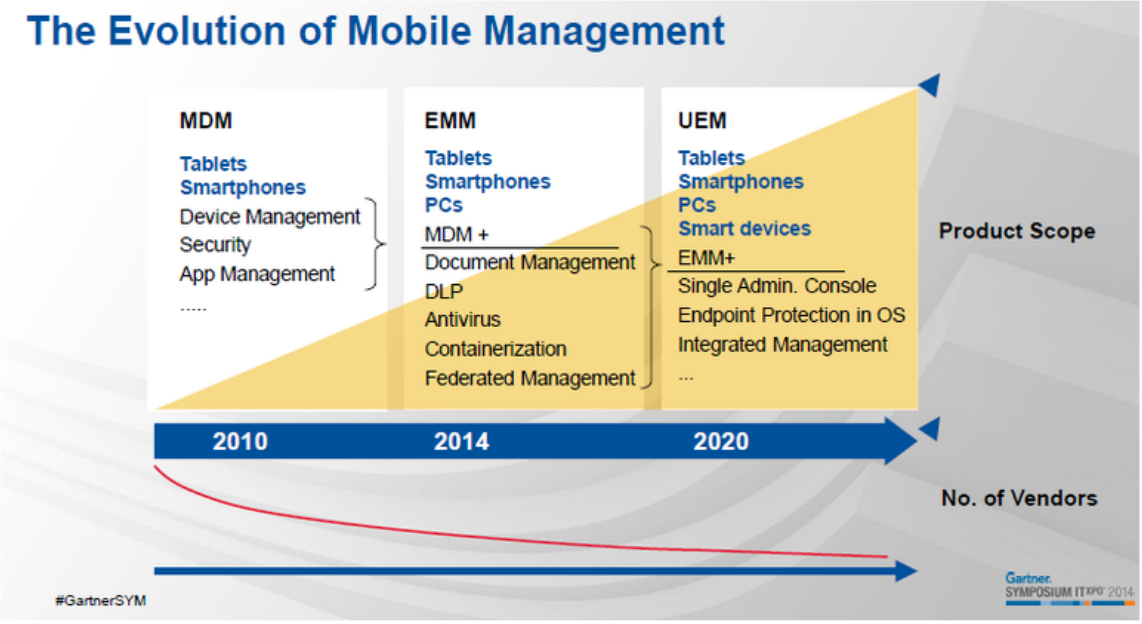
MCM by navíc měla definovat soubor zásad pro přístup k datům a kontrolu a monitorování neoprávněného přístupu. Zatímco Mobile Asset Management a Mobile Application Management se zaměřuje na zabezpečení mobilních zařízení a aplikací, MCM zajišťuje bezpečnou výměnu souborů mezi mobilními koncovými body. V této souvislosti poskytuje MCM mobilním aplikacím data nezbytná k začlenění do místní infrastruktury informačních technologií. MCM spolupracuje s Mobile Application Management. Na aplikační vrstvě poskytuje Mobile Application Management potřebnou kontrolu nad mobilními aplikacemi, které jsou využívány pro změnu a smazání. Mobile Content Management slouží jako prostředník k poskytování obsahu a informací aplikační vrstvě na vysoce zabezpečené úrovni. Tyto dva přístupy zajišťují soulad s předpisy týkajícími se zákona o ochraně osobních údajů. Detailnější informace jsou dostupné zde [2].

2.4.4 Mobile Security Management

Mobile Security Management (dále jen MSM) je osvědčený postup k ochraně a ověřování mobilních uživatelů. MSM je odpovědný za prosazování zásad registrovaných mobilních zařízení. Účelem MSM je omezit nebo povolit definovanou úroveň nastavení v celém prostředí. Záměrem správy mobilního zabezpečení je navíc konfigurace a implementace kontrolních opatření, ověřování integrity a detekce hrozeb a slabin. Když organizace plánuje implementovat strategii podnikové mobility, musí vzít v úvahu správu mobilních aplikací (Mobile Application Management), správu mobilních zařízení (MDM), správu mobilního obsahu (MCM) a správu mobilního zabezpečení (MSM). Tyto čtyři oblasti je třeba vzájemně propojit, aby byla garantovaná přesná úroveň zabezpečené podnikové mobility. MSM nelze tedy považovat za izolovanou část. V rámci přístupu a výše uvedených záměrů definuje MSM zásady a opatření mobilních zařízení pro všechny čtyři oblasti a umožňuje systému reagovat na změny. Podrobněji se o tomto tématu píše zde [2].

2.4.5 Shrnutí rozdílných nástrojů

Jak tedy mobilita kráčela vpřed, transformovala také způsob, jakým jsme pracovali a žili, technologie a platformy se začaly komplikovat. Výsledkem je, že se řešení MDM transformovala na řešení Enterprise Mobility Management (EMM). Opět s exponenciálním nárůstem mobilních aplikací objevily inovativní způsoby spolupráce a přístupu k podnikovým zdrojům bez ohledu na čas a místo. Nyní tedy nešlo jen o kontrolu a dohled nad zařízeními, ale také o maximalizaci produktivity kancelářské a vzdálené pracovní síly s přísným zabezpečením. Řešení EMM rozšířilo možnosti IT na



Obrázek 2.3: Rozdíly v samotných řešení, převzato z [6]

aplikační a informační úrovni, obvykle nasazené s MDM (správa mobilních zařízení), MAM (Mobile Application Management), MCM (správa mobilního obsahu) a MSM (Správa zabezpečení mobilních zařízení).

Platí, že se zvýšením množství typů zařízení koncových uživatelů, nazývanými koncové body, se správa a zajištění zabezpečení vyvinuly na Unified Endpoint Management (UEM). Koncové body v podniku dnes zahrnují širokou škálu zařízení a operačních systémů, počínaje od stolních počítačů po mobilní zařízení a dokonce i zařízení IoT. UEM však není jen o udělení nebo odepření přístupu, ale zahrnuje správu zařízení, zabezpečení zařízení, řízení přístupu, správu uživatelů, doručování aplikací a jejich aktualizaci.

Stručně řečeno, UEM je nedávné oživení softwarových aplikací pro správu, monitorování, zabezpečení a řízení všech druhů mobilních zařízení koncových uživatelů v podnikovém prostředí. Vyvinul se ze Mobile Device Management na Enterprise Mobility Management a nyní na Unified Endpoint Management. Tento vývoj je zaměřen výhradně na poskytnutí svobody uživatelům při používání jejich vlastních zařízení a na zajištění společnosti, že jejich zaměstnanci mají přístup k podnikovým datům, aplikacím a dalším prostředkům v zabezpečeném prostředí.

Tyto tři řešení jsou si velice podobné, nejstarší je samotné MDM, viz. obrázek 2.3. V roce 2014 se objevuje na trhu název EMM a během 4 let několik EMM řešení změnilo název na UEM. Více o tomto tématu je napsáno v kapitole 2.5, která se věnuji americké společnosti Gartner. EMM vstupuje do popředí a MDM se stalo jakousi podmnožinou samotného EMM řešení, které v sobě obsahuje komplexnější řešení pro správu mobilních zařízení.

2.5 Historie řešení pro mobilní zařízení

Společnost Gartner, Inc. je americká analytická společnost působící v oboru informačních technologií, která se zaměřuje na výzkumné a poradenské činnosti. Byla založena v roce 1979 a svoji působnost rozšířila v zemích po celém světě. Při své analytické činnosti dbá na to, aby neupřednostňovala žádného dodavatele, produkt či službu. Výzkumné zprávy Gartner vyjadřují stanovisko této analytické organizace a žádné ze zkoumaných řešení není následně doporučováno.

Obrázek 2.4: Magický kvadrant z roku 2011, převzato z [7]

Při pohledu na vývoj analýz v oblasti Mobile Device Managementu za období od roku 2011 je vidět, že řešení od společností Airwatch, Citrix (Zenprise) a MobileIron jsou v porovnání s ostatními produkty hodnoceny dlouhodobě nejlépe a jsou zařazovány do kvadrantu vůdčích řešení na trhu. V roce 2011 se poprvé objevuje výzkum, který ukazuje první vydání magického kvadrantu v oblasti MDM, viz obrázek 2.4. Z více než 100 společností, které provádí nějakou správu mobilních zaří-

zení, bylo vybráno 23 společností. Mezi vedoucí prodejce na trhu se ve zprávě dostali MobileIron, AirWatch, Good Technology a Sybase.

Obrázek 2.5: Magický kvadrant z roku 2014, převzato z [7]

V roce 2014 se společnost Gartner rozhodla změnit kategorii na Enterprise Mobility Management Suites, kvůli rozšíření využití technologie, která se z obyčejné základní správy mobilních zařízení přesunula do správy jak zařízení, tak jejího obsahu a aplikací, viz obrázek 2.5. Tím se snížil počet společností z 18, které byly v minulém magickém kvadrantu, na 14 společností. Na obrázku níže je 5 lídrů MobileIron, AirWatch, IBM, Citrix a Good Technology. IBM a Citrix se zde dostali po zakoupení společností Fiberlink a Zenprise, kteří v letech 2012 a 2013 byli na pozici lídrů.

Obrázek 2.6: Magický kvadrant z roku 2018, převzato z [7]

V roce 2018 je opět možnost vidět změnu kategorie z Enterprise Mobility Management Suites na Unified Endpoint Management Tools, viz obrázek 2.6. Důvodem provedené změny bylo rozšíření počtu operačních systémů, které nynější řešení pro správu podporují. V roce 2018 je 5 lídrů, IBM jak jsem již zmiňoval se zde dostala po zakoupení společnosti Fiberlink. Společnosti VMware a BlackBerry se zde dostaly po zakoupení společností AirWatch a Good Technologies. Pouze společnosti Microsoft a MobileIron si vydobyly cestu skrze lídry na trhu.

2.6 Přehled řešení pro správu mobilních zařízení

Většina řešení pro vzdálenou správu mobilních zařízení jsou cloudového typu. Základní správu MDM a EMM nabízí hned několik poskytovatelů, zatímco UEM řešení nabízí většinou větší poskytovatelé, jako jsou IBM, Microsoft, Citrix a podobné mezinárodní společnosti. Všichni poskytovatelé softwarů nabízí prakticky stejnou základní správu pro mobilní zařízení ve svém řešení. Poskytovatelé se snaží získat nějakou výhodu nad ostatními poskytovateli tím, že implementují komplexnější řešení, například umělou inteligenci, monitorování firemní sítě a diagnózu abnormálního chování v síti. Po výběru řešení budete nuceni si stáhnout na zařízení klientskou aplikaci, která bude se zařízením komunikovat.

2.6.1 IBM

IBM je americká mezinárodní technologická společnost se sídlem ve státě New York. Byla založena v roce 1911. MaaS360 je řešení od společnosti IBM, které se zabývá správou mobilních zařízení. Jde o plně integrovanou SaaS službu, která se dlouhodobě umisťuje ve výzkumu Gartner v kvadrantu lídrů. Jedná se o přístup Unified Endpoint Management. Řešení bylo původně vyvinuté společností Fiberlink Communications, až do jeho získání společností IBM. IBM využila výhody svého širokého softwarového portfolia ke kombinování produktu MaaS360 s přilehlými produkty IBM v oblastech, jako je ochrana před mobilními hrozbami (MTD), informace o zabezpečení a správě událostí (SIEM) a identita jako služba (IDaaS), k řešení několika souvisejících funkcí v jediný produkt. Společnost IBM navíc využila své odborné znalosti Watson AI k poskytování analytických řešení, která zákazníkům pomáhají identifikovat a třídit problémy se zařízeními spravovanými MaaS360. Engine Watson jako umělá inteligence, která hledá chyby v řešení a analyzuje data, aby chybám předešla, se jeví jako vysoce užitečná z pohledu Gartner. MaaS360 se rozděluje na 4 cenové kategorie, které se platí měsíčně. Nejlevnější Essentials varianta začíná na 4 dolarech za zařízení bez zdanění. Nejdražší forma nese název Enterprise a za jedno zařízení se měsíčně platí 9 dolarů bez zdanění. Je zde možnost vyzkoušet si Enterprise verzi na 30 dní zdarma. Další informace ohledně IBM řešení jsou ve zprávách od Gartner nebo na oficiálních stránkách prodejce [8, 9].

- Výhody IBM MaaS360 with Watson
  - Umělá inteligence, která hledá zranitelnosti v koncových zařízeních.
  - Lídr v tomto odvětví.
  - Kompletní podpora mobilních operačních systémů.
  - Dlouholeté zkušenosti v oblasti správy zařízení.
- Nevýhody IBM MaaS360 with Watson

  - Neexistuje místní řešení. Nicméně řešení nabízí místní přístupovou bránu pro e-mail a další aplikace.

2.6.2 Headwind Solutions Ltd.

Headwind Solutions Ltd. je ruská společnost se sídlem ve městě Petrohrad. Společnost byla založená v roce 2008. Headwind MDM je název MDM řešení, které je zaměřeno na operační systém Android. Společnost se zaměřuje hlavně na mobilní zařízení, která vlastní firma, tedy zařízení COPE a COBO. Řešení nijak neodděluje pracovní a osobní prostor. MDM server je poskytován jako open source software v Community a Enterprise verzi. Řešení se rozděluje na tři kategorie Community, Professional a Enterprise. Community verze je bezplatná, ale chybí ji funkce, které jsou ve verzích Professional a Enterprise. V Professional verzi není místní řešení, takže se jedná čistě o cloudové řešení, které stojí 1,65 dolarů za zařízení měsíčně. Enterprise verze má všechny funkce, ale platí se za kompletní řešení. Cena kompletního řešení je 1990 dolarů včetně jednoho roku podpory od společnosti Headwind Solutions. Detailnější informace o rozdílech mezi verzemi jsou k nalezení zde [10].

- Výhody Headwind MDM
  - Zaměření na menší a střední podniky
  - Možnost zakoupit si celý produkt a případně k tomu dokupovat podporu od společnosti Headwind Solutions.
- Nevýhody Headwind MDM
  - Nevhodné pro osobní zařízení.
  - Málo funkcí pro osobní zařízení, chybí funkce, které v sobě zahrnují řešení EMM od ostatních dodavatelů.

2.6.3 Citrix

Citrix je americká mezinárodní technologická společnost se sídlem ve státě Florida. Společnost byla založena v roce 1989 a poskytuje široké portfolio z oblasti virtualizace a cloudu. Citrix Endpoint Management je řešení od společnosti Citrix. Jedná se o cloudovou službu, která se zabývá správou mobilních zařízení. Dlouhodobě se objevuje v roční zprávě od Gartner v kvadrantu lídrů, kromě nejnovější zprávy z roku 2020, kde Citrix řešení bylo umístěno do kvadrantu specializovaného segmentu. Citrix nabízí celou sadu funkcí pro správu koncových bodů pro širokou škálu operačních platforem, od mobilních a počítačových zařízení až po zařízení IoT, jedná se totiž o řešení UEM. Řešení Citrix Endpoint Management zůstává vhodné pro organizace s existující investicí do virtualizační technologie Citrix a pro ty, kteří používají Citrix ShareFile. Citrix také nabízí místní řešení.

Citrix Endpoint Management se rozděluje na 3 cenové kategorie, nejlevnější je Stand-Alone za 4 dolary za uživatele nebo za 3 dolary za zařízení. Workspace Premium stojí 18 dolarů za uživatele a za Workspace Premium Plus se platí 25 dolarů za uživatele. Cena za jedno zařízení klesá s narůstajícím počtem zařízení. Citrix Workspace nabízí přímou integraci a snadno aplikovatelné řešení pro správu zařízení i virtualizaci aplikací v rámci jedné hlavní konzole, přes kterou se spravují a ovládají aplikace a jejich obsah. Je zde také možnost vyžádat si demo. Další informace ohledně Citrix řešení jsou ve zprávách Gartner nebo na oficiálních stránkách prodejce [8, 9].

- Výhody Citrix Endpoint Management
  - Některé funkce od Citrix Endpoint Management jsou kompatibilní s řešením Intune od společnosti Microsoft. Je vhodné, pokud už společnost vlastní licence na Microsoft Intune.
  - Je obecně vhodný pro společnosti, které už nějaké řešení od Citrix mají.
  - Kompletní podpora mobilních operačních systémů.
  - Dlouholeté zkušenosti v oblasti správy zařízení.
- Nevýhody Citrix Endpoint Management
  - Menší zaměření na menší podniky.
  - Kvůli provázaným produktům a licencím od společnosti Citrix, budoucí klienti, kteří nemají žádnou infrastrukturu od společnosti Citrix nebo ji neplánují mít, by měli zvážit jiného dodavatele.

2.6.4 Ivanti

Ivanti je americká společnost, která sídlí ve státě Utah. Společnost byla založena v roce 1985 a patří mezi dodavatele IT softwaru v oblasti bezpečnosti a správy systému. Řešení od společnosti Ivanti se jmenuje MobileIron UEM, které bylo zakoupeno v září roku 2020 od společnosti MobileIron. Ivanti také vlastní druhé řešení Ivanti UEM. Co se týče MobileIron UEM, tak zde je možnost mít kromě cloudového řešení i místní řešení. MobileIron UEM se dlouhodobě umisťuje v kvadrantu lídrů. Řešení je vhodné pro společnosti, které hledají kompletní správu mobilních zařízení. K MobileIron UEM je také dodávaný software Pulse Secure, který zabezpečuje data v BYOD, COPE a CYOD zařízeních. Řešení se rozděluje na dva typy Secure UEM a Secure UEM Premium, kdy každá z těchto dvou variant má jiné funkce. Jedna z nevýhod tohoto řešení je, že místní a cloudové řešení má rozdílné funkce. MobileIron UEM nemá pevně stanovenou cenu za zařízení nebo za uživatele. Secure UEM verzi je možné si vyzkoušet na 30 dní zdarma. Další informace ohledně MobileIron řešení jsou ve zprávách Gartner nebo na oficiálních stránkách prodejce [8, 9].

- Výhody MobileIron UEM

  - Lídr v tomto odvětví.
  - Dlouhodobé zkušenosti v oblasti správy zařízení.
  - Kompletní podpora mobilních operačních systémů.

- Nevýhody MobileIron UEM

  - Rozdílné verze cloudového a místního řešení, nemají stejné funkce a aktualizace nevycházejí zároveň.

2.6.5 Samsung

Samsung je největší mezinárodní technologická společnost v Jižní Koreji, která sídlí ve městě Soul. Společnost byla založena v roce 1969 a patří mezi největší výrobce a dodavatele spotřební elektroniky na světě. Řešení od společnosti Samsung se jmenuje Samsung Knox Manage a jde o cloudovou platformu. Samsung Knox Manage nemá místní řešení. Řešení se zaměřuje hlavně na Mobile Application Management (MAM) a Mobile Security Management (MSM). Samsung Knox Manage je řešení pro různé platformy, ale je optimalizované pro zařízení Samsung, díky tomu nabízí toto řešení spoustu výhod, včetně správy mobilních zařízení a jejich podporu pro zařízení od společnosti Samsung. Toto EMM řešení lze získat jedině přes jiné distributory, než je samotný Samsung. Podobně funguje i podpora tohoto řešení, a to skrze partnery nebo distributory. Je zde možnost zakoupení celého balíčku s názvem Knox Suite. Stejně tak, jako Knox Manage, je zde dodáno i řešení Mobile Enrollment, E-FOTA a Knox Platform for Enterprise. Mobile Enrollment slouží k automatické registraci do firemní sítě, jakmile zaměstnanec zapne zařízení a připojí se k síti. E-FOTA slouží k vzdálené aktualizaci operačního systému a zabezpečení zařízení bez interakce se zaměstnancem. Knox Platform for Enterprise nabízí doslova vojenské zabezpečení telefonů, tabletů a hodinek Tizen od společnosti Samsung. Detailnější informace o Samsung Knox Manage jsou k nalezení zde [11].

- Výhody Samsung Knox Manage

  - Zaměření na bezpečnost (Mobile Security Management) a oddělení osobních dat od firemních (Mobile Application Management).
  - Dlouhodobé zkušenosti se správou zařízení.

- Nevýhody Samsung Knox Manage

  - Podpora přes distributory nebo partnery.
  - Neexistuje místní řešení.
  - Zakoupit řešení nelze jiným způsobem, než přes distributory nebo partnery.

2.6.6 Zoho Corporation

Zoho Corporation je mezinárodní indická společnost, která sídlí ve městě Chennai. Společnost byla založena v roce 1996 a zabývá se vývojem softwaru. Řešení od Zoho Corporation se nazývá ManageEngine Mobile Device Manager. Toto UEM řešení nabízí jak cloudové, tak místní řešení. ManageEngine Mobile Device Manager může být součástí Desktop Central, což je UEM nástroj pro celkovou správu pracovních stanic, mobilních zařízení a serverů. ManageEngine se dlouhodobě objevoval v roční zprávě od společnosti Gartner, kromě nejnovější zprávy z roku 2020. Řešení od této společnosti je především vhodné pro menší a střední organizace, které hledají základní funkce EMM nebo MDM řešení. Velká výhoda je možnost zdarma využívat řešení pro 25 zařízení jak v cloudové, tak v místní verzi. Řešení se rozděluje na 3 kategorie, Free, Standard a Professional. Rozdíly jsou k nalezení zde [12]. Ceny u místního a cloudového řešení se liší. Standard verze stojí u místního řešení 12 dolaru a 16 dolaru u cloudového řešení za rok. Verze Professional stojí u místního řešení 22 dolaru a u cloudového řešení 30 dolaru za rok.

- Výhody ManageEngine Mobile Device Manager
  - Vhodné pro menší a střední firmy.
  - Verze zadarmo pro 25 zařízení.
  - Místní i cloudové řešení.
- Nevýhody ManageEngine Mobile Device Manager
  - Rozdíl mezi cloudovým a místním řešením.

2.6.7 Tabulkový přehled řešení

Tabulka 2.1: Přehled cen

Ceny	MaaS360	Headwind	Citrix	Samsung	MobileIron	ManageEngine
Měsíčně za zařízení	$4-9	$1,65	$3,20-5	$1,93	$4-7,5	$1-1,83 | $1,33-2,5 *
Měsíčně za uživatel	$8-18	-	$3,80-6,25	-	$6-12	-
Verze zadarmo	NE	ANO	NE	NE	NE	ANO
Zkušební verze	30 dní	120 dní	30 dní	90 dní	30 dní	30 dní

* Rozdíl mezi cloudovým řešením a místním řešením.

Tabulka 2.2: Rozdílné funkce

Funkce	MaaS360	Headwind	Citrix	Samsung	MobileIron	ManageEngine
Místní řešení	✗	✓	✓	✗	✓	✓
Cloudové řešení/SaaS	✓	✓	✓	✓	✓	✓
Posílání zpráv do zařízení	✓	✓	✓	✓	✓	✓
Samsung Knox	✓	✓	✓	✓	✓	✓
Kiosk režim	✓	✓	✓	✓	✓	✓
Vzdálené ovládání	✓	$590	✓	✓	✓	✓
Zamknutí zařízení	✓	✓	✓	✓	✓	✓
Resetování zařízení	✓	✓	✓	✓	✓	✓
GPS lokace	✓	✓	✓	✓	✓	✓
Firemní obchod	✓	✗	✓	✓	✓	✓
Zakázání aplikaci	✓	✓	✓	✓	✓	✓
Povolení aplikaci	✓	✓	✓	✓	✓	✓
Aktualizace aplikaci	✓	✓	✓	✓	✓	✓
Alarm	✓	✓	✓	✓	✓	✓
Zasílání dokumentu do zařízení	✓	✓	✓	✓	✓	✓
Technické detaily o zařízení	✓	✓	✓	✓	✓	✓
Podpora Android Enteprise	✓	✗	✓	✓	✓	✓

Kapitola 3

Výběr vhodného řešení pro operační systém Android

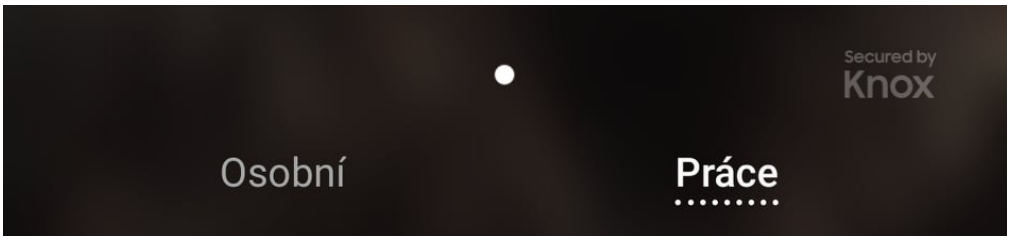
Nelze přímo říci, které řešení pro Android je vhodné, a které není. Zvolit správné řešení pro firmy obnáší podrobnou analýzu. Aby bylo zvolené řešení správné, je nutné položit si základní otázky. Firma by si měla určit jaké jsou její potřeby a kritéria pro volbu. Více v kapitole 3.2.

3.1 Android

Android je mobilní operační systém, u kterého je využito jádro operačního systému Linux. Najdeme ho v chytrých telefonech, tabletech a v chytrých televizích. Android je open source projekt, který původně vyvíjela firma Android Inc. V roce 2005 firmu zakoupila společnost Google. V roce 2007 se následně založila firma Open Handset Alliance (OHA), která patří mezi sdružení výrobců telefonů, komponentů a operátorů, kteří se podílejí na vývoji platformy Android. Android má největší zastoupení v mobilních zařízeních jak u tabletu, tak u chytrých telefonů.

3.1.0.1 Android Enterprise

Android Enterprise je Google platforma pro správu Android zařízení [13]. Jedná se o sadu rozhraní pro správu zařízení skrze API (Application Programming Interface), které jsou zabudované v operačním systému Android. Tyto rozsáhlé funkce zabezpečení a správy se nachází ve všech zařízeních Android 5.0 a výše. Nezáleží tedy, který upravený typ operačního systému Androidu máme, jelikož Android Enterprise sjednocuje správu systému Android a tím odstraňuje varianty výrobců a nabízí pro všechna zařízení stejné funkce správy. Problém může nastat pokud zařízení nemá službu Google Mobile Services (GMS), jako například některá zařízení Huawei. Tato technologie funguje na zařízeních Android a umožňuje vnucení a nastavení programů tak, aby zařízení splňovalo standardy firemního prostředí. Android Enterprise umožňuje správu zařízení v různých scénářích, které se dělí



Obrázek 3.1: Rozdělení pracovního a osobního prostoru

na Work profile neboli Profile owner a Fully managed device neboli Device owner. Work profile neboli pracovní profil je vhodný pro typy zařízení, jako jsou BYOD, COPE a CYOD. Tento scénář oddělí pomocí kontejneru pracovní a osobní prostor a tím zabezpečuje firemní data na osobních zařízeních, aniž by bylo ohroženo soukromí zaměstnanců. Device owner neboli vlastník zařízení je nejlepší typ scénáře pro správu zařízení vlastněných firmou, jako jsou typy zařízení COPE, COBO a CYOD. Ve srovnání s pracovním profilem poskytuje tento scénář administrátorům MDM větší kontrolu nad nastavením zařízení, což usnadňuje zabezpečení zařízení a dat.

Android Enterprise je vyžadovaný pro některá řešení, povolit se dá prostřednictvím spravované domény G Suite nebo novější metodou skrze spravovaný účet Google. Android Enterprise není nijak zpoplatněn, pokud máte licenci k některému EMM řešení. Seznam řešení, které podporují Android Enterprise, je k nalezení zde [14]. Jak vypadá rozdělení osobního a pracovního prostředí, lze vidět na obrázku zde 3.1.

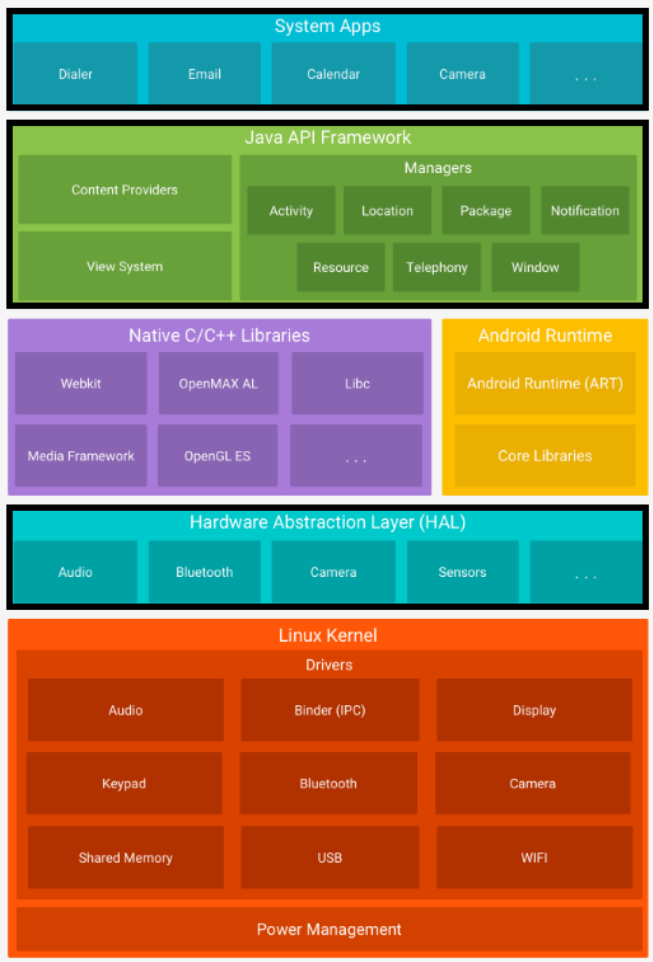
Existuje seznam Android zařízení, která jsou doporučovaná firmou Google pro správu mobilních zařízení ve firemním prostředí u Android Enterprise, seznam zařízení lze najít zde [15].

3.1.0.2 Zero-touch enrollment

Zero-touch enrollment je proces, kdy je na zařízení nainstalovaná správa zařízení, jakmile jej zaměstnanec spustí. Zařízení čeká na první spuštění a připojení k internetu, pokud zařízením byla přidělená firemní správa, inicializují se stažení aplikací, politiky a další firemní nastavení. Tento proces umožňuje rychlou a snadnou registraci velkého množství mobilních zařízení Android. Zařízení se automaticky zaregistrují, jakmile se zaměstnanec přihlásí k internetu. Výhoda tohoto procesu je, že se nemusí zařízení ručně registrovat. Zařízením je nastavený profil Device Owner. Podobný proces využívá aplikace Samsung Knox Enrollment.

3.1.1 Architektura operačního systému Android

Architektura operačního systému Android je rozdělena na šest částí, jak lze na obrázku 3.2 vidět. Android Enterprise komunikuje skrze tuto architekturu prostřednictvím tři komponent. První komponenta je konzole EMM v softwaru, který administrátor spravuje. Další komponenta je Android Device Policy, což jsou zásady nebo politiky, které určuje firma svým zaměstnancům na jejich zařízeních. Třetí komponenta je samotný spravovaný firemní obchod Google Play.



Obrázek 3.2: Architektura operačního systému Android, převzato z [16]

3.1.1.1 Linux Kernel

Linux Kernel je jádro operačního systému Android. Jedná se o nejnižší vrstvu této architektury. Android Runtime spoléhá na jádro pro její funkcionalitu, jako je například správa paměti, správa sítí, zabudované ovladače nebo správy procesů, například souběžného běhu aplikací, které běží jako samostatné procesy s oprávněním stanoveným systémem. Použití linuxového jádra umožňuje využití důležitých funkcí zabezpečení a výrobcům zařízení umožňuje vyvíjet ovladače pro Android. [16]

3.1.1.2 Hardware Abstraction Layer(HAL)

Hardwarová abstraktní vrstva (HAL) poskytuje standardní rozhraní, které odhalují možnosti hardwaru zařízení na vyšší úrovně Java API rámce. Tato abstraktní vrstva se skládá z několika knihovních modulů, z nichž každá implementuje rozhraní pro konkrétní typ hardwarové komponenty, například kamera nebo technologie bluetooth. [16]

V této části komunikuje Android Enteprise s hardwarovými komponenty, díky Android Management API, která je součástí Android Enterprise, lze na tyto komponenty zasílat příkazy.

3.1.1.3 Native C/C++ Libraries

Další část jsou knihovny, které jsou psané v programovacím jazyce C a C++, tyto knihovny jsou využívaný základními komponentami pro operační systém Android. Platforma Android poskytuje toto rozhraní vývojářům skrze API. Například knihovna Media Libraries podporuje přehrávání video a audio formátů, knihovna SQLite je relační databáze, knihovna FreeType pro renderování bitmapových a vektorových fontů. Tyto knihovny patří mezi základní knihovny v této vrstvě. [16]

3.1.1.4 Android Runtime

Většina aplikací na Androidu je psána v jazyce Java nebo v jazyce Kotlin. U Android verze 5.0 a výše je provozována každá aplikace ve svém vlastním procesu a se svou vlastní instancí, které se říká Android Runtime (ART). Důvody použití ART je úspora energie a další výrazné zrychlení aplikací. ART je designován pro spouštění více virtuálních strojů na zařízeních s nízkou pamětí, spuštěním souborů DEX, což je formát bajtkódu, který je optimalizován pro minimální paměťové nároky. [16]

3.1.1.5 Java API Framework

Celá sada funkcí operačního systému Android je k dispozici vývojářům prostřednictvím rozhraní API napsaných v jazyce Java. [16]

V této části lze najít Android Enterprise, který komunikuje s ostatními částmi systému.

3.1.1.6 System Apps

Nejvyšší vrstvou této architektury jsou systémové aplikace. Využívají ji uživatelé, jde například o sadu základních aplikací pro e-mail, zasílání SMS zprávy, kalendáře, internetový prohlížeč, kontakty a další předinstalované aplikace. [16]

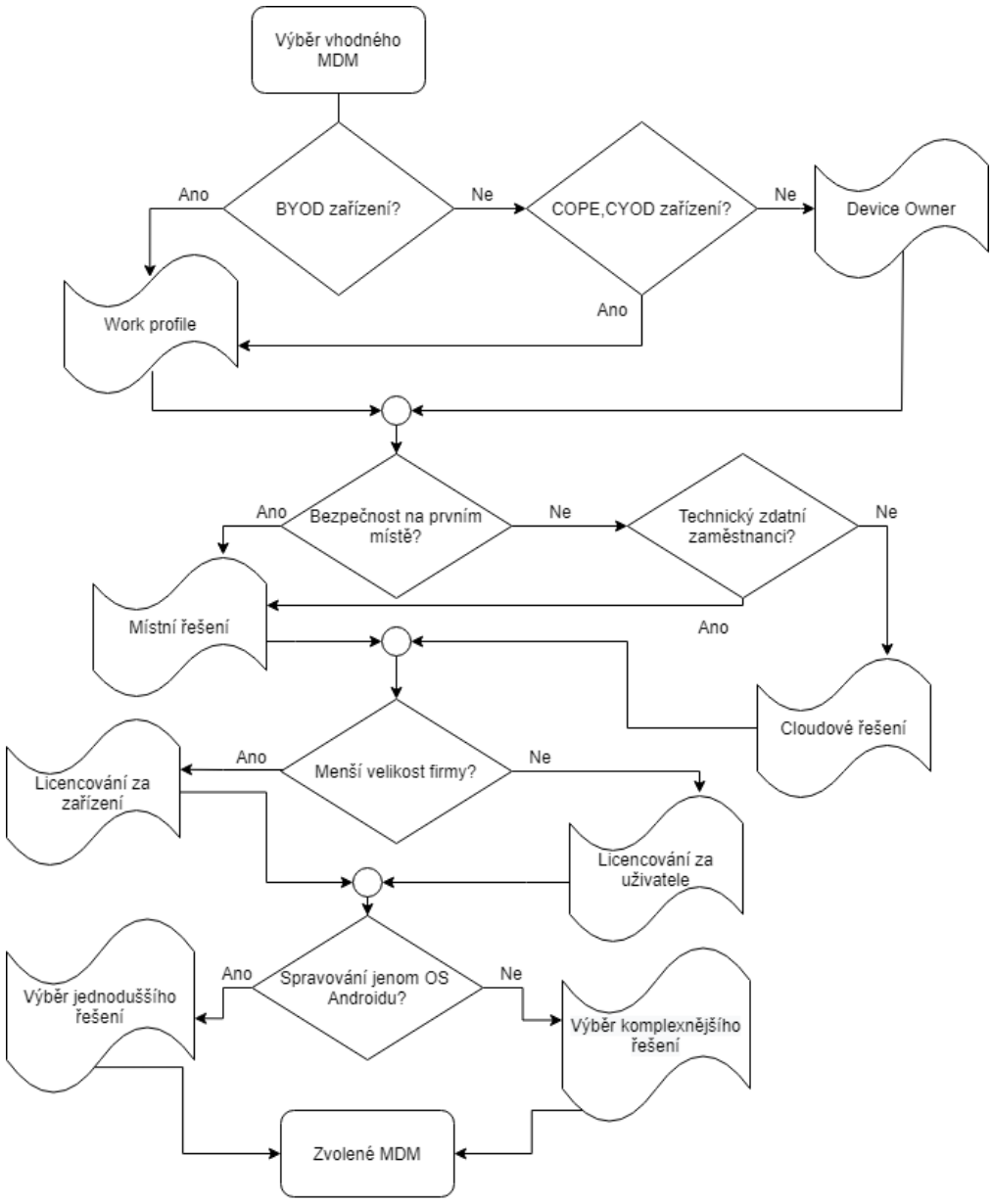
V této části si Android Enterprise vytváří vlastní oddělené systémové aplikace od soukromých systémových aplikací, jde například o Google Play, kontakty, internetový prohlížeč nebo složky.

3.2 Výběr vhodného MDM řešení pro mobilní operační systém Android

Proces rozhodování jaké MDM zvolit, si můžeme ulehčit zodpovězením následujících otázek.

- Jakou implementaci zvolíme?
  - Zde je možnost mezi místním a cloudovým řešením. Implementace místního řešení bude vyžadovat hardware a technicky schopné zaměstnance, aby tento typ implementace realizovali a také ho spravovali. Správné nastavení firemní sítě, nastavení firewallů, provádění bezpečnostních aktualizací a monitoring sítě, všechny tyto funkce musí zaměstnanci zvládnout. Pokud firma tuto implementaci zvládne, bude mít MDM řešení plně pod kontrolou. [17]
  - Cloudové řešení nezahrnuje starost o MDM server. Není tedy potřeba technicky zdatných lidí, kteří se o MDM server budou starat. Měsíční náklady jsou větší a je zde bezpečnostní riziko, jelikož data se budou pohybovat mimo firmu bez jakékoliv kontroly. MDM server není hardwarově náročný. U menší firmy do 500 zařízení bude stačit takový server, který má alespoň 4 GB RAM, 10 GB volného místa a alespoň dvoujádrový procesor.
- Bude společnost povolovat zaměstnancům využití osobního zařízení pro pracovní účely (BYOD)?
  - Pokud ano, MDM řešení by tedy mělo podporovat Android Enterprise pro rozdělení osobního a pracovního prostoru.
- Pokud společnost nebude povolovat zařízení BYOD. Bude povolovat zařízení typu COPE a CYOD?
  - Rozdělení osobního a pracovního prostoru je vhodné i u těchto zařízení COPE a CYOD, které budeme moct použít pro osobní účely. Android Enterprise umí vytvořit ve scénáři Device owner prostředí pro osobní účely tak, jak tomu je v případě pracovního profilu.
- Jaký typ licence si zvolíme?
  - Zde je možnost provádět platbu za počet zařízení, počet uživatelů, kteří souběžně využívají více mobilních zařízení nebo zakoupení celého softwaru. Licencování za zařízení je vhodnější pro menší podniky. Naopak licencování podle počtů uživatelů je vhodnější pro větší firmy, kvůli náročnosti evidence každého zařízení. Počáteční investice u zakoupení celého softwaru je vyšší, ale z dlouhodobého hlediska bude levnější. [17]
- Bude zaměstnavatel spravovat pouze operační systém Android?
  - Zaměstnavatel by měl uvažovat dopředu. Je možné, že bude chtít spravovat i zařízení s operačním systémem Windows nebo iOS.

- Má zaměstnavatel zařízení, které podporují Samsung Knox? Je pro zaměstnavatele na prvním místě zabezpečení firemních dat?
  - Samsung Knox patří mezi nejpokročilejší bezpečnostní implementace na mobilních zařízeních, co se týče zabezpečení firemní správy. Společnost Gartner porovnává různá zabezpečení na různých zařízeních a Samsung Knox zde dlouhodobě mívá vysoké hodnocení. Tabulkový přehled z roku 2019, je k nalezení zde [18]. Originální výzkum od společnosti Gartner je k nalezení zde [19].



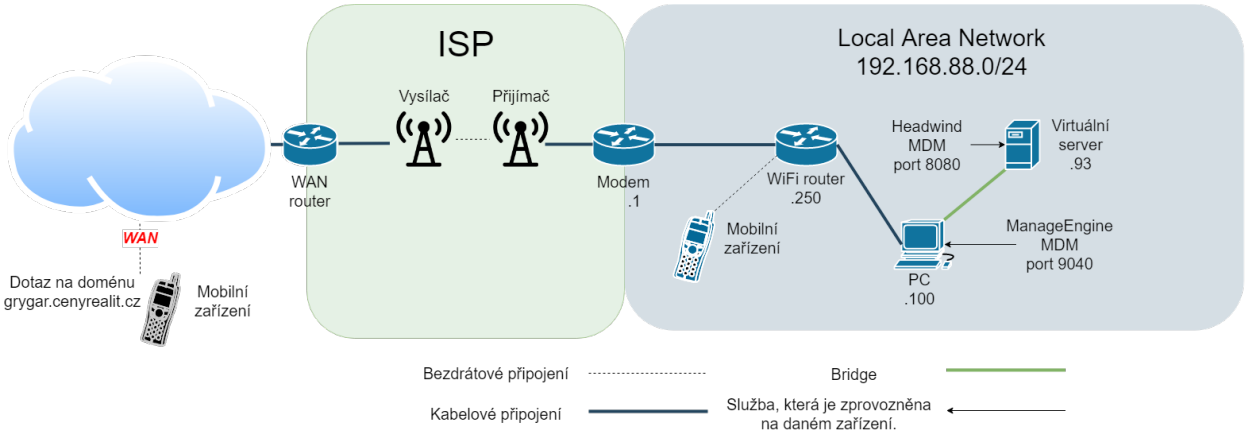
Obrázek 3.3: Vývojový diagram výběru MDM

Kapitola 4

Instalace a konfigurace různých MDM řešení

Testovaná zařízení jsou Samsung Galaxy S9+, Sony Xperia X, Google Pixel 3a XL, OnePlus 7T a Huawei P40 Pro.

Vybrané programy pro testovaní jsou IBM MaaS360 with Watson, Samsung Knox Manage, Headwind MDM a ManageEngine MDM. Schéma připojení pro Headwind MDM a ManageEngine MDM je na obrázku 4.1.



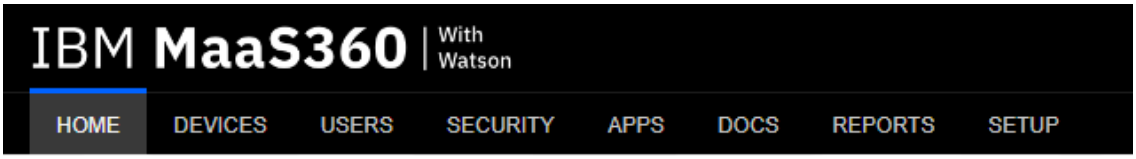
Obrázek 4.1: Schéma zapojení místního MDM řešení

4.1 IBM MaaS360 with Watson

MaaS360 lze získat skrze oficiální stránky IBM. Po výběru produktu MaaS360 je možnost zvolit si zkušební verzi po dobu 30 dní. Jediný požadavek pro získání produktu je firemní email. Není tedy možnost vyzkoušet si IBM řešení přes takzvané freemaily (google.com nebo seznam.cz). Vyřízení žádosti je automatické, takže se nemusí čekat na potvrzení žádosti o bezplatnou verzi. Důvodem zvolení tohoto řešení bylo vybrání alespoň jednoho softwaru, který se dlouhodobě objevuje ve výzkumu od společnosti Gartner.

4.1.1 Administrátorské rozhraní MaaS360

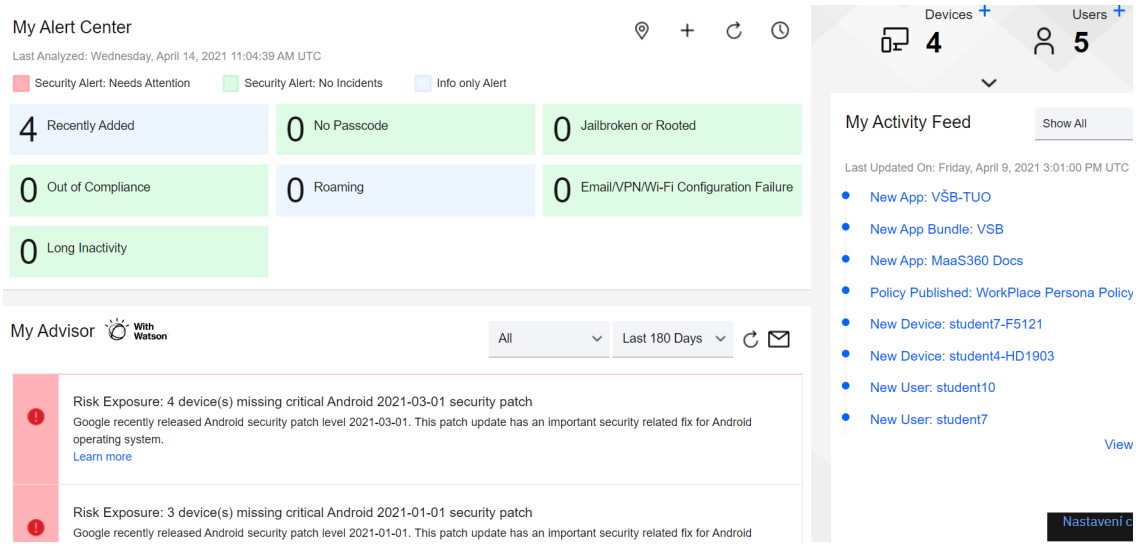
Po přihlášení do MaaS360 se administrátor dostane do rozhraní pro vzdálenou správu. Na obrázku 4.2 je vidět, že se rozhraní rozděluje na Home, Devices, Users, Security, Apps, Docs, Reports a Setup.



Obrázek 4.2: MaaS360 navigace

Home

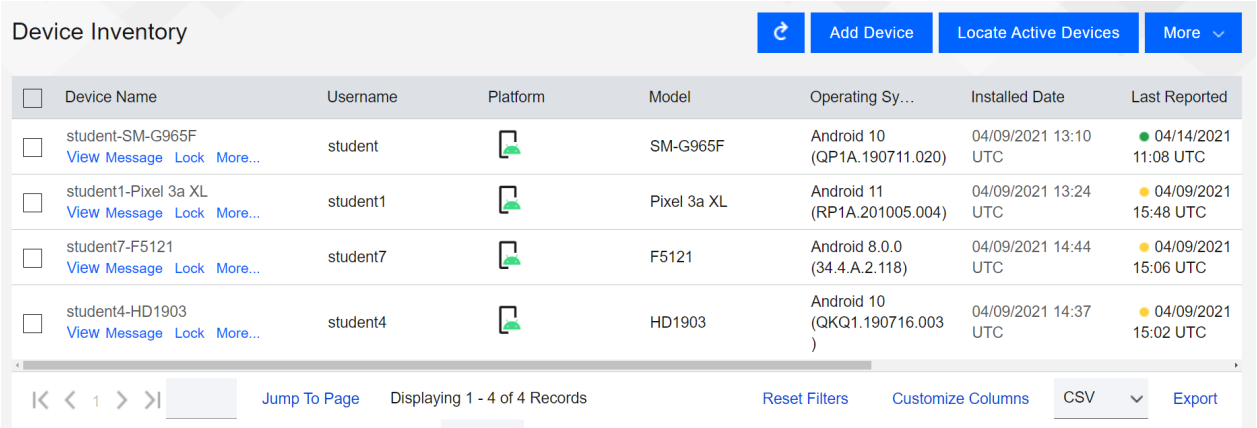
- Po kliknutí na Home se administrátorovi zobrazí úvodní stránka s jednoduchým přehledem, jak lze na obrázku 4.3 vidět.
- Administrátor zde vidí:
  - rady od umělé inteligence Watson, nová rizika, které mohou nastat, neaktualizované nebo nestabilní zařízení,
  - výstražné centrum, které administrátora upozorňuje na případné problémy se zabezpečením nebo informace, které zobrazují změny v prostředí a
  - počet zařízení a uživatelů v MaaS360.



Obrázek 4.3: MaaS360 Home

Devices

- V této záložce vidí administrátor všechna zařízení. Zde může administrátor spravovat a nastavovat mobilní zařízení, které do MaaS360 přidal, viz obrázek 4.4. V tomto rozhraní lze také vytvořit skupinu zařízení a odesílat na tuto skupinu různé příkazy.
- Po zaškrtnutí boxu u příslušného mobilního zařízení, může administrátor vydávat například následující příkazy pro mobilní zařízení:
  - úplné vymazání dat na mobilním zařízení,
  - zaslání notifikací na zařízení,
  - zamknutí telefonu,



Obrázek 4.4: MaaS360 Device

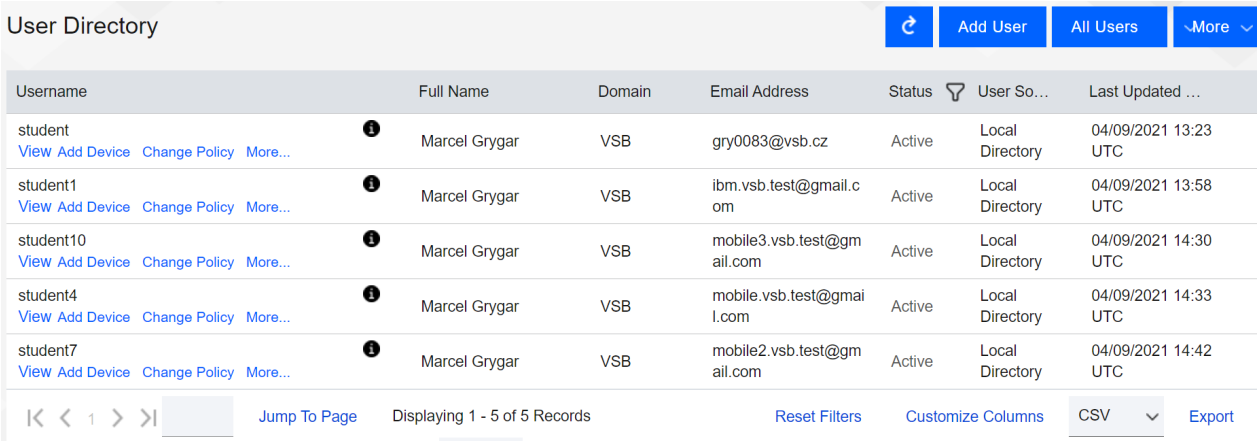
- změnu vlastnictví,
- distribuci aplikace na zařízení,
- distribuci dokumentu na zařízení,
- změnu zásad pro zařízení,
- odstranění zařízení z MDM,
- spuštění alarmu,
- vytvoření skupiny telefonů,
- zjištění lokace a
- změnu pravidel pro zařízení.

Users

- V nabídce Users, může administrátor vytvořit pro každého zaměstnance uživatelský účet. Je zde vidět přehled všech uživatelů, viz obrázek 4.5. Lze zde vytvářet skupinu uživatelů, mazat uživatele, měnit jejich politiku, deaktivovat je nebo jim resetovat heslo. Je zde možnost vytvářet i skupinu zařízení, pro které platí stejné možnosti jako u uživatele.

Security

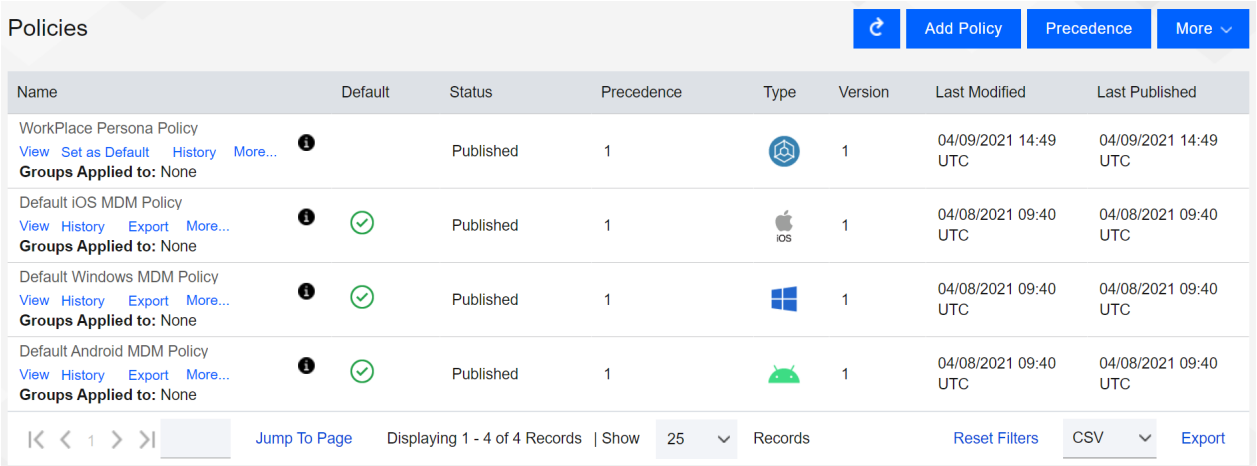
- V této záložce může administrátor vytvářet politiku pro zařízení nebo uživatele, viz obrázek 4.6. Tato politika má své pravidla, není možné omezovat některé funkce zařízení, které nepatří pod firmu. Při vytváření politiky může administrátor nastavit například následující možnosti:
  - nakonfigurování hesla pro přístup do pracovního prostoru,
  - zakázání nebo povolení odemykaní zařízení skrze otisku prstu, rozpoznání obličeje, očních sítnic,



Obrázek 4.5: MaaS360 Users

  - přenos USB, ladění skrze USB, připojení fyzického média,
  - povolení snímání obrazovky, povolení obnovy do továrního nastavení,
  - konfigurování zakázaných aplikací a povolených aplikací,
  - blokování určitých adres a povolení určitých adres na prohlížeči,
  - neustále připojení k VPN a nakonfigurování WiFi,
  - konfigurování tapety,
  - vynucení aktualizací a
  - zakázání kamery, povolení ztlumení mikrofonu a úpravu hlasitosti a další.

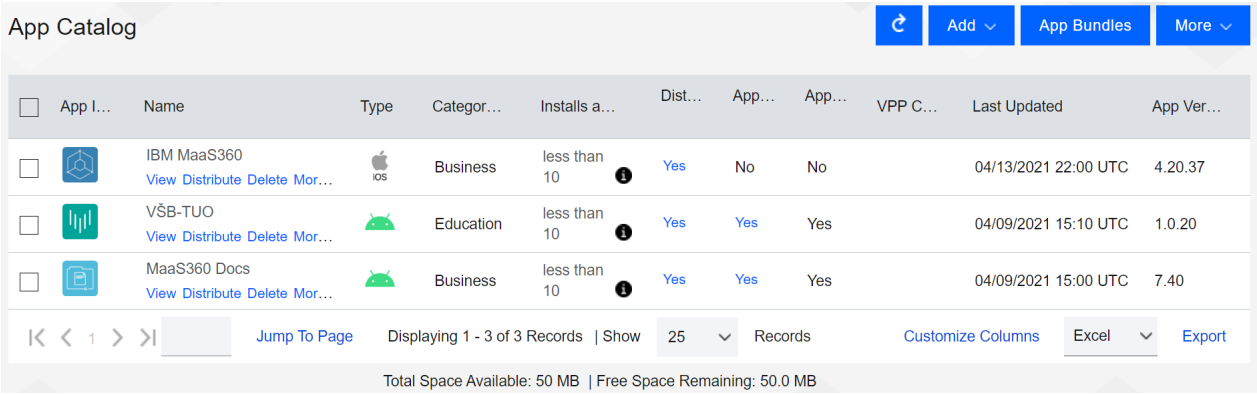
- Pro zařízení s Knox implementací jsou zde i další možnosti, jako je zakázání a nahrávání zvuku, nahrávání kamerou, nastavení časového limitu na WiFi, nastavení limitu mobilních dat, zakázání NFC a podobně.



Obrázek 4.6: MaaS360 Security

Apps

- Zde má možnost administrátor povolovat a zakazovat určité typy aplikací z obchodů, viz obrázek 4.7. Pro administrátora je zde taky možnost poslat na zařízení aplikaci, která není v obchodu. Existuje možnost zabalit více aplikací do balíčků a pracovat s němi jako se skupinou. Baliček lze upravovat, distribuovat na různé uživatele nebo zařízení a lze je smazat.



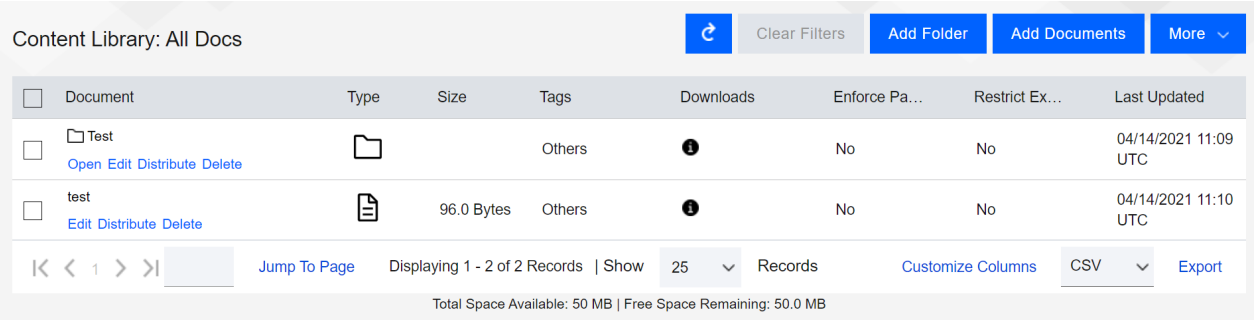
Obrázek 4.7: MaaS360 Apps

Docs

- V nabídce Docs může administrátor vytvářet hierarchii složek a zasílat dokumenty na zařízení. Z obrázku 4.8 lze vidět, které složky a soubory jsou na zařízeních. Při přidání složky lze nastavit například:
  - komu bude složka na zařízení přiřazena,
  - zakázání otevírání složky pomocí jiných aplikací,

- stahování pouze z WiFi technologie,
- okamžité stahování,
- chránění složky heslem a
- zakázání smazání složky.

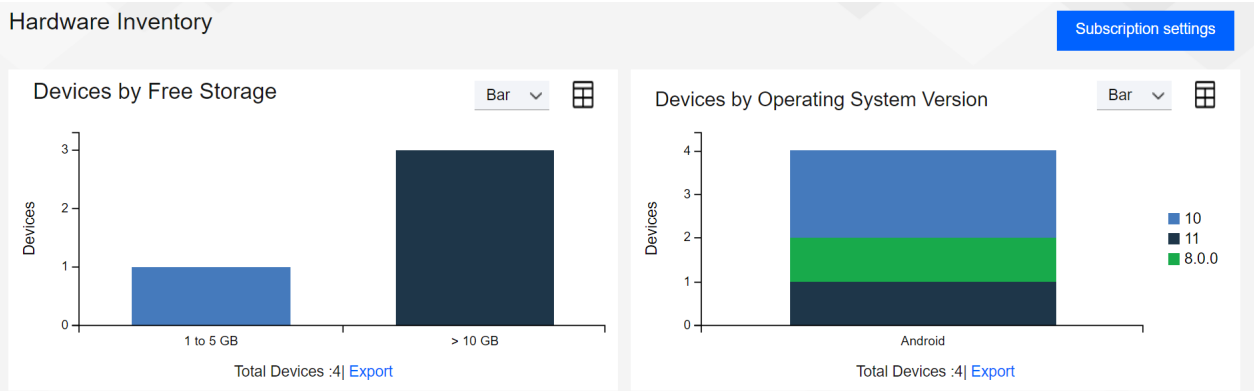
- Při přidání dokumentu lze nastavit podobné pravidla, jako u složky, navíc je zde mazání, úprava a vyjmutí dokumentu.



Obrázek 4.8: MaaS360 Docs

Reports

- Zde administrátor vidí přehlednou statistiku o mobilních zařízeních, které jsou připojené k řešení MaaS360. Grafy je možné si nastavit například na výsečový graf. Na obrázku 4.9 jsou verze operačního systému Android, které jsou připojené k Maas360.



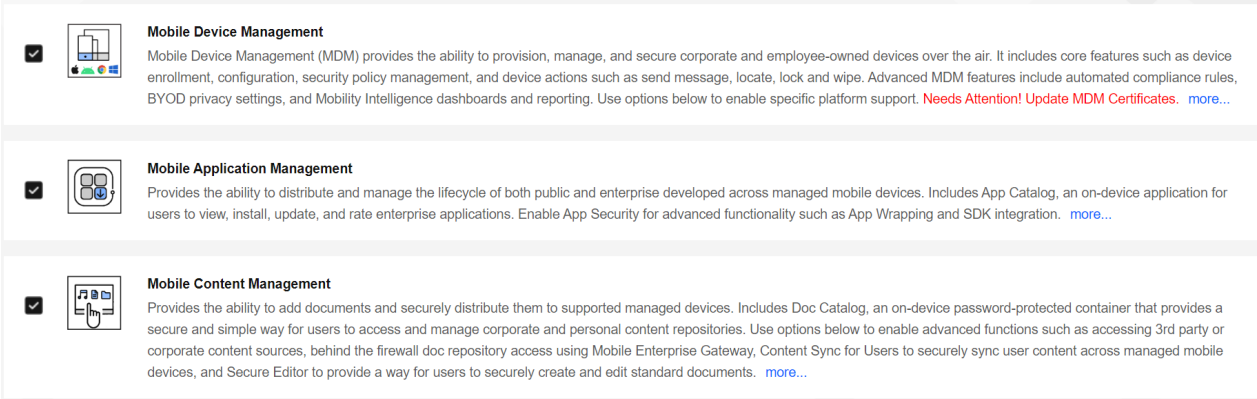
Obrázek 4.9: MaaS360 Reports

Setup

- V záložce Setup může administrátor konfigurovat nastavení služeb nebo přidat další administrátory, kteří budou spravovat zařízení. Nastavení MDM, Mobile Application Management

(MAM) a MCM se nachází v této záložce, viz obrázek 4.10. Dále může administrátor nastavit tyto například služby:

- zabezpečení pošty,
- zabezpečení prohlížeče,
- MaaS360 VPN pro přístup k podnikové sítí,
- vzdálenou podporu pro mobilní zařízení,
- správu notebooku a stolních počítačů,
- integraci podnikového emailu,
- Enterprise Gateway pro přístup k informačním zdrojům za bránou firewallu a
- aktivování portálu pro zaměstnance, přes který si můžou zařízení spravovat.

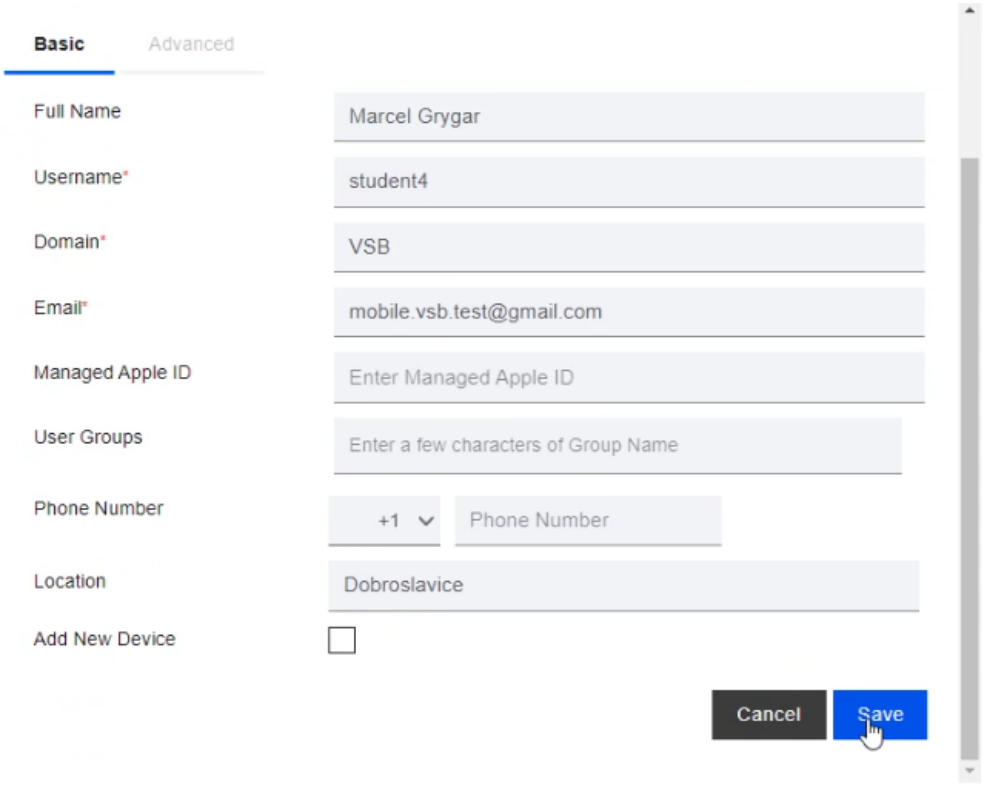


Obrázek 4.10: MaaS360 Setup

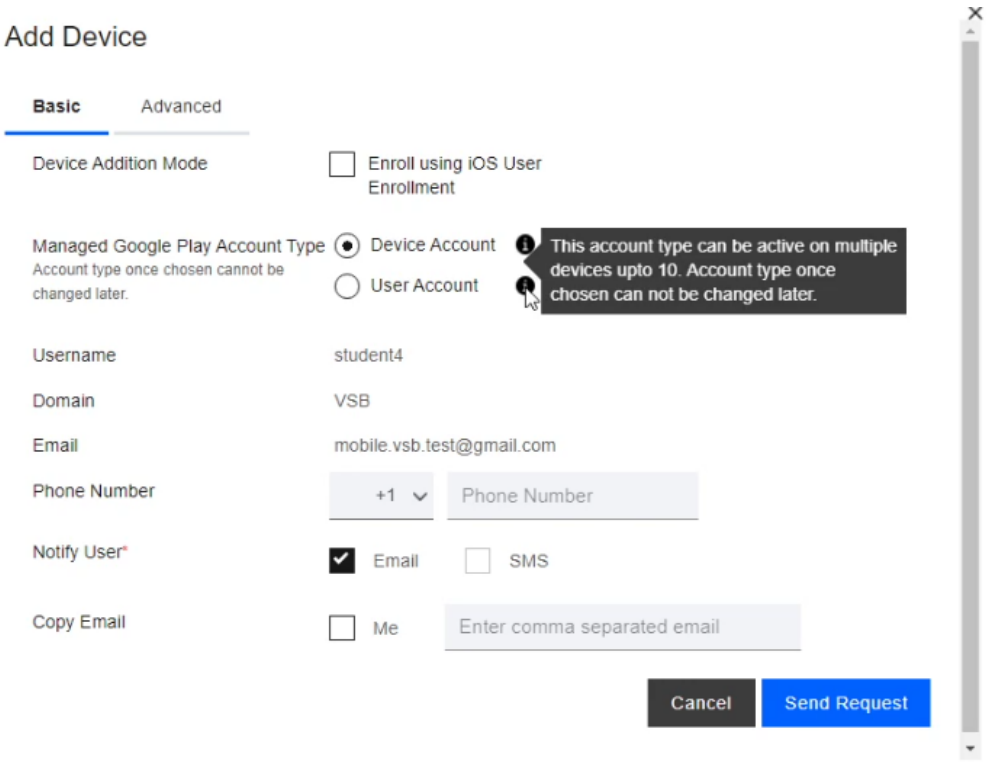
4.1.2 Připojení zařízení k řešení MaaS360

Pro připojení Android zařízení bude muset administrátor zprovoznit Google administrátorský účet. Po kliknutí na tlačítko Setup v rozhraní se objeví různé nastavení služeb. Zde si administrátor rozklikne možnost Mobile Device Managment, viz obrázek A.4. MaaS360 upozorní, že není aktivovaný Android Enterprise, zde jsou dvě možnosti, jak aktivovat Android Enterprise pomocí Google administrátorského účtu. První možnosti je aktivování skrze G Suite pomocí EMM Provider tokenů. Druhá možnost je bez G Suite pomocí Android Enterprise Standalone. Pokud společnost nevlastní G Suite, nezbývá společnosti nic jiného, než zvolit Android Enterprise Standalone, viz obrázek A.3.

Aby administrátor mohl zařízení přidat do MaaS360, bude muset přidat zaměstnance, kterému zařízení bude patřit. To udělá tak, že přejde do nabídky Users přes navigaci a zde si zvolí Add User, viz obrázek 4.11.



Obrázek 4.11: MaaS360 přidání zaměstnance v nabídce Device



Obrázek 4.12: MaaS360 přidání zařízení v nabídce Users

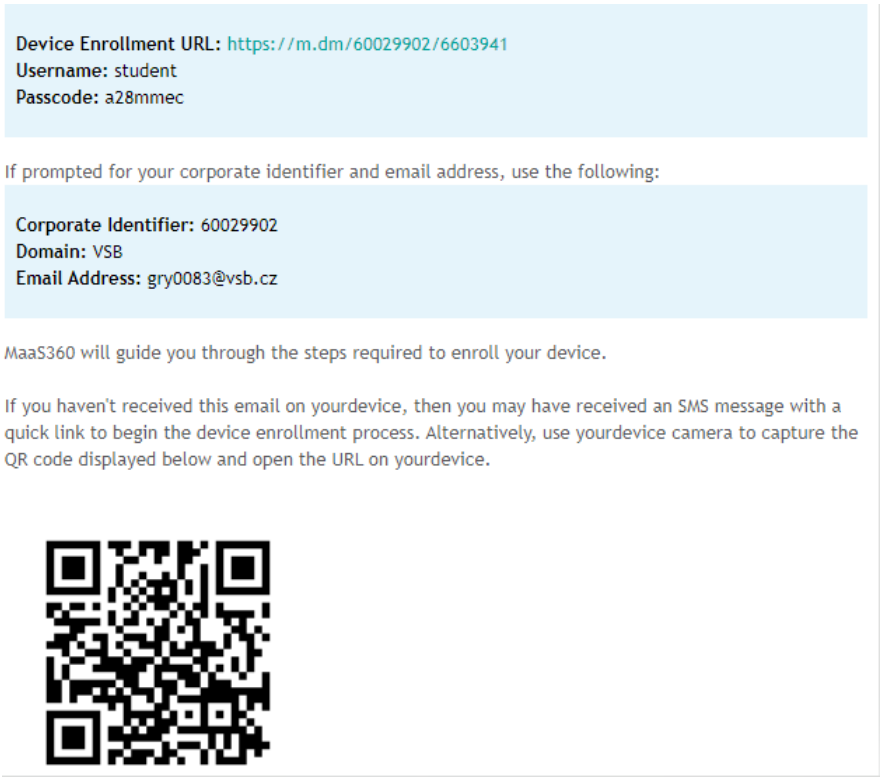
V nabídce Users může administrátor zůstat a rovnou přidat uživateli zařízení pomocí tlačítka Add Device. Na obrázku 4.12 je vidět, co musí administrátor vyplnit, aby zařízení přidal do MaaS360.

Po registrování zařízení přijde zaměstnancům email nebo SMS zpráva, že zařízení bylo přidáno a vyžaduje nainstalování aplikace, která bude komunikovat se serverem. Zaměstnanec si stáhne do zařízení aplikaci z obchodu s aplikacemi (Google Play). Formulář z emailu lze vidět na obrázku 4.13. Po stažení aplikace musí zaměstnanec zadat přihlašovací údaje, aby zařízení registroval do MaaS360, po registraci se mu nastaví profil Work Profile. Viz obrázek 4.14. Pro profil Device Owner je nutné zařízení resetovat do továrního nastavení a aktivovat QR skener. QR kód administrátor najde pod rozhraním Setup. QR skener se aktivuje pomocí 6 kliknutí na úvodní obrazovce po resetování zařízení.

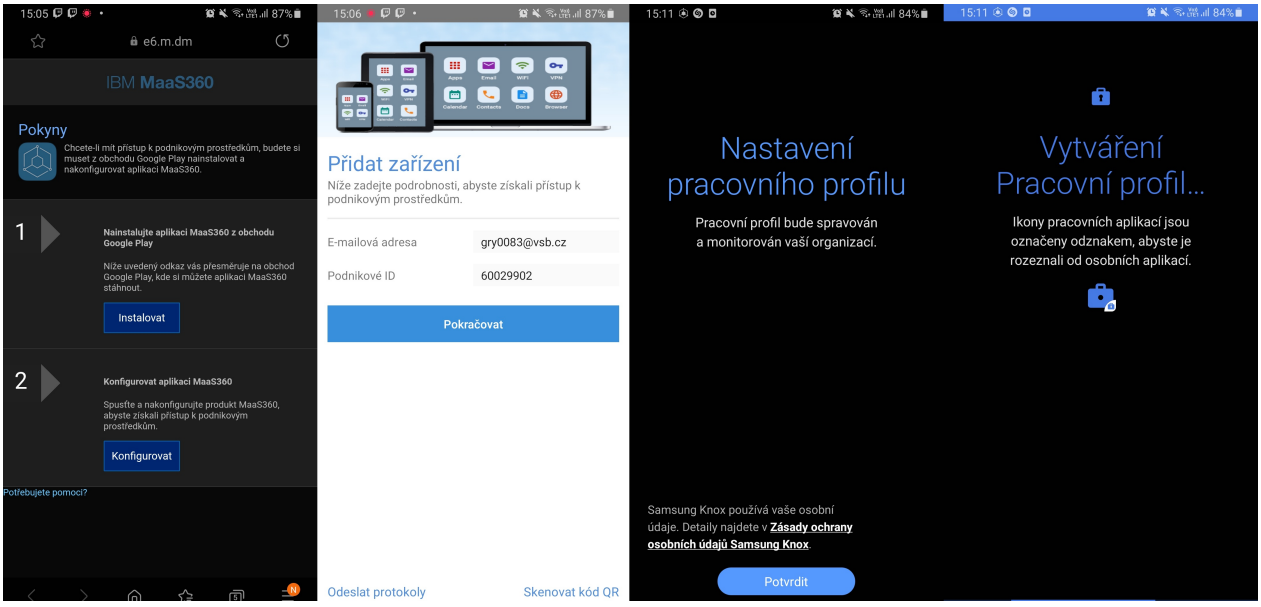
4.1.3 Testování funkčnosti MaaS360

Z důvodu absence Google Mobile Services (GMS) nebylo možné otestovat zařízení Huawei, viz obrázek A.1.

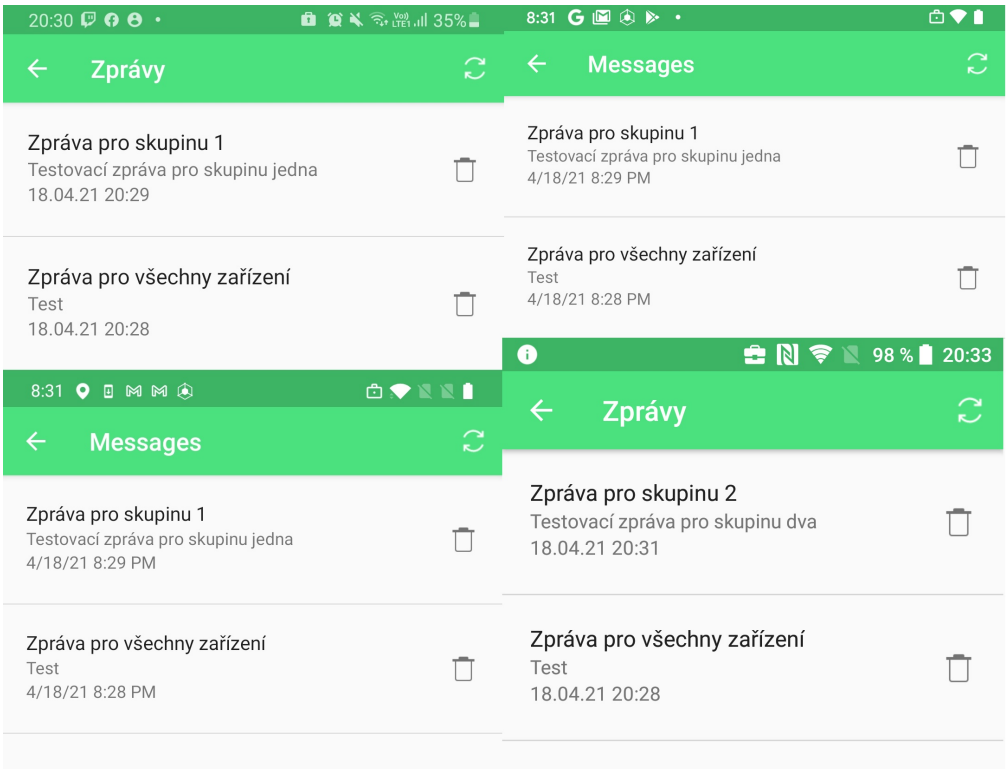
Pro otestování funkčnosti MaaS360 jsem zvolil následující scénář. Poslal jsem na všechna zařízení zprávu, potom jsem zařízení rozdělil na skupiny a poslal zprávy na dané zařízení skrze skupinu.



Obrázek 4.13: MaaS360 přihlašovací údaje



Obrázek 4.14: MaaS360 instalace

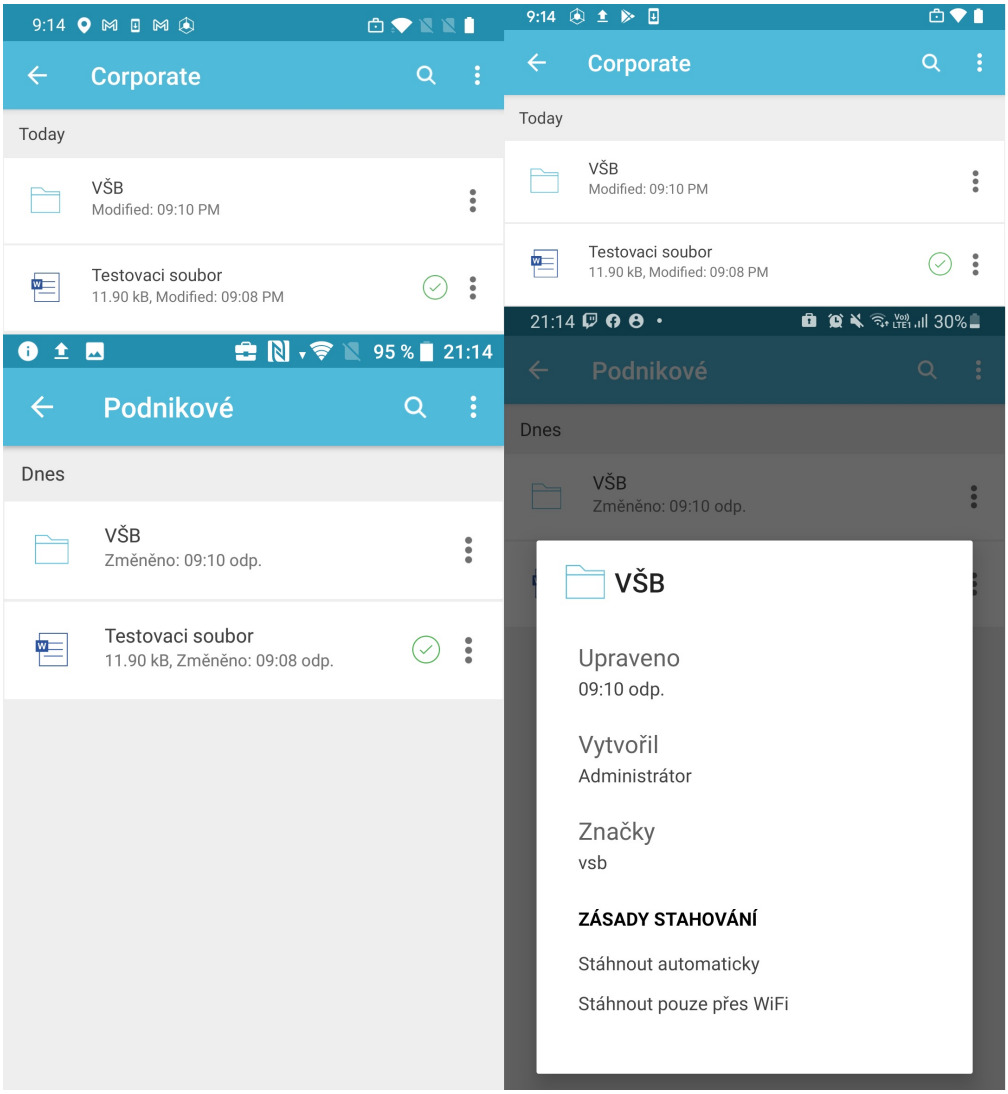


Obrázek 4.15: MaaS360 odeslané zprávy na zařízeních

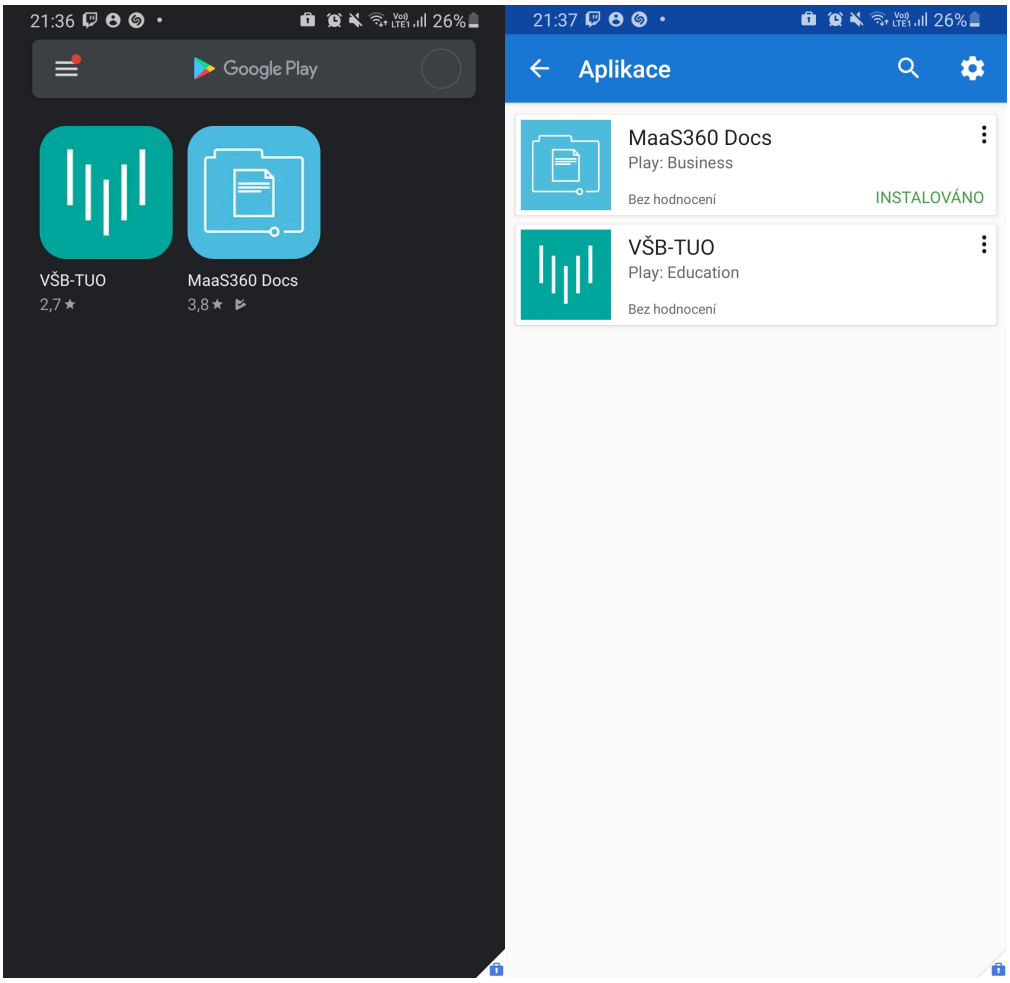
Dalším krokem bylo vytvoření složky na všech zařízeních a následně distribuce souboru. Posledním krokem bylo vytvoření podnikového obchodu s povolenými aplikacemi.

K odeslání zprávy musí administrátor přejít do nabídky Devices. Po zakliknutí všech zařízení může administrátor poslat zprávu. Zpráva se následně objeví v zařízení jako notifikace a zapíše se do prostředí MaaS360 v aplikací zpráv. Pro odeslání zpráv pro dané skupiny musí administrátor vytvořit skupinu, do které přiřadí zařízení nebo uživatele, to může udělat přes záložku Devices nebo Users. Zprávy na zařízení potom najde uživatel v pracovním prostředí pod aplikací zprávy, viz obrázek 4.15.

U vytvoření složky musí administrátor otevřít rozhraní Docs a zde kliknout na možnost Add Folder. V tomto rozhraní administrátor zůstane a vytvoří přes možnost Add Documents soubor, který bude distribuovat. Po vytvoření příkazu uvidí zaměstnanec ve svém zařízení v aplikaci Docs složku a soubor, viz obrázek 4.16.



Obrázek 4.16: MaaS360 distribuovaný soubor a složka



Obrázek 4.17: MaaS360 firemní obchod a seznam aplikací

Přidání aplikací do firemního obchodu musí administrátor provést skrze záložku Apps. Zde si vyhledá přes Google Play aplikace, které chce přidat. V mém případě to jsou aplikace MaaS360 Docs a VŠB-TUO. Jak vypadá firemní obchod a seznam aplikací, které jsou povolené, lze vidět na obrázku 4.17.

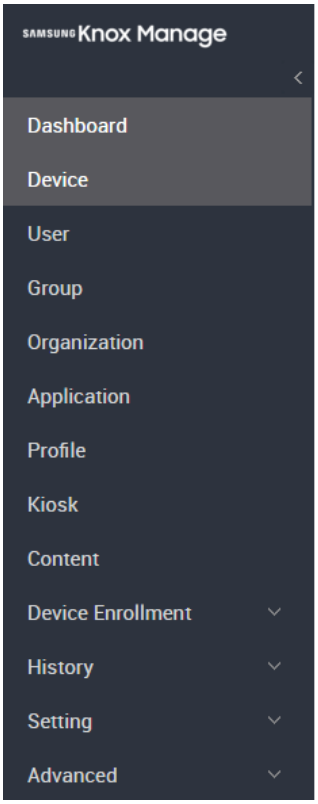
Testování proběhlo v pořádku s menšími problémy. Ne všem zařízením přišla notifikace, ale zpráva v aplikaci byla k zobrazení. Co se týče prodlevy mezi příkazy, tak u zaslání zpráv na zařízení, došla zpráva v rámci pár sekund. U zprávy přes skupiny byla prodleva delší a u některých zařízení se objevila až po aktualizaci aplikace. U složky a dokumentu byl příkaz vykonán hned. Přístup k aplikacím ve firemním obchodu byl povolen v rámci pár vteřin a aplikace se objevily hned po příkazu.

4.2 Samsung Knox Manage

Na oficiální stránce Samsungu Knox lze získat Samsung Knox Suite, který obsahuje i Samsung Knox Manage, tato licence je zdarma po dobu 90 dní a je limitována pro 30 zařízení. Pro získání je nutné vlastnit firemní email. Vyřízení žádosti o licenci trvá krátkou dobu. Důvodem zvolení softwaru bylo najít ve správě MDM rozdíly u zařízení Samsung, oproti ostatním zařízením.

4.2.1 Administrátorské rozhraní Samsung Knox Manage

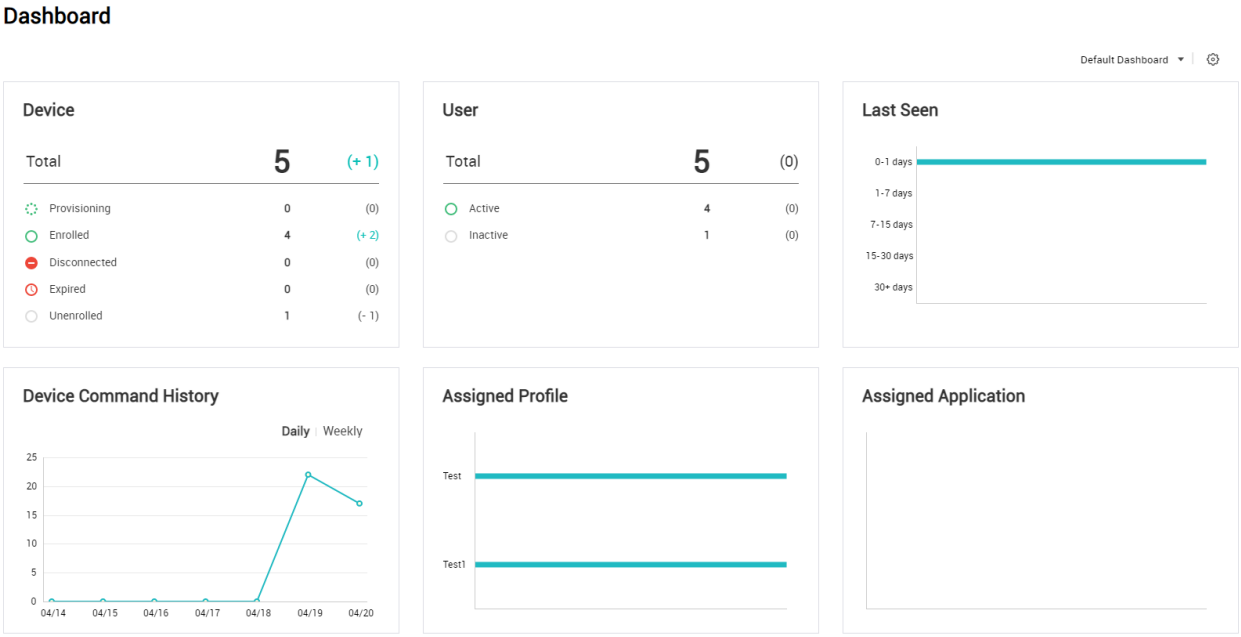
Jakmile se administrátor přihlásí do Samsung Knox Manage, zobrazí se mu vodorovné rozhraní na levé straně. Rozhraní se rozděluje na Dashboard, Device, User, Group, Organization, Application, Profile, Kiosk, Content, Device Enrollment, History, Setting, Advanced, viz obrázek 4.18.



Obrázek 4.18: Samsung Knox Manage navigace

Dashboard

- V tomto rozhraní vidí administrátor přehled o zařízeních a uživatelích, viz 4.19. Je zde vidět aktivita, historie příkazu, informace o licenci, a jaký typ operačního systému je v tomto EMM softwaru.



Obrázek 4.19: Samsung Knox Manage Dashboard

Device

- V této záložce vidí administrátor seznam všech zařízení. U zařízení jsou vidět podrobnosti, jestli je na zařízení nastaveno Work Profile nebo je celé zařízení spravované EMM serverem. Po zaškrtnutí boxu u zařízení je možné pomocí tlačítka Device Command vyslat do zařízení příkazy, viz obrázek 4.20.

User

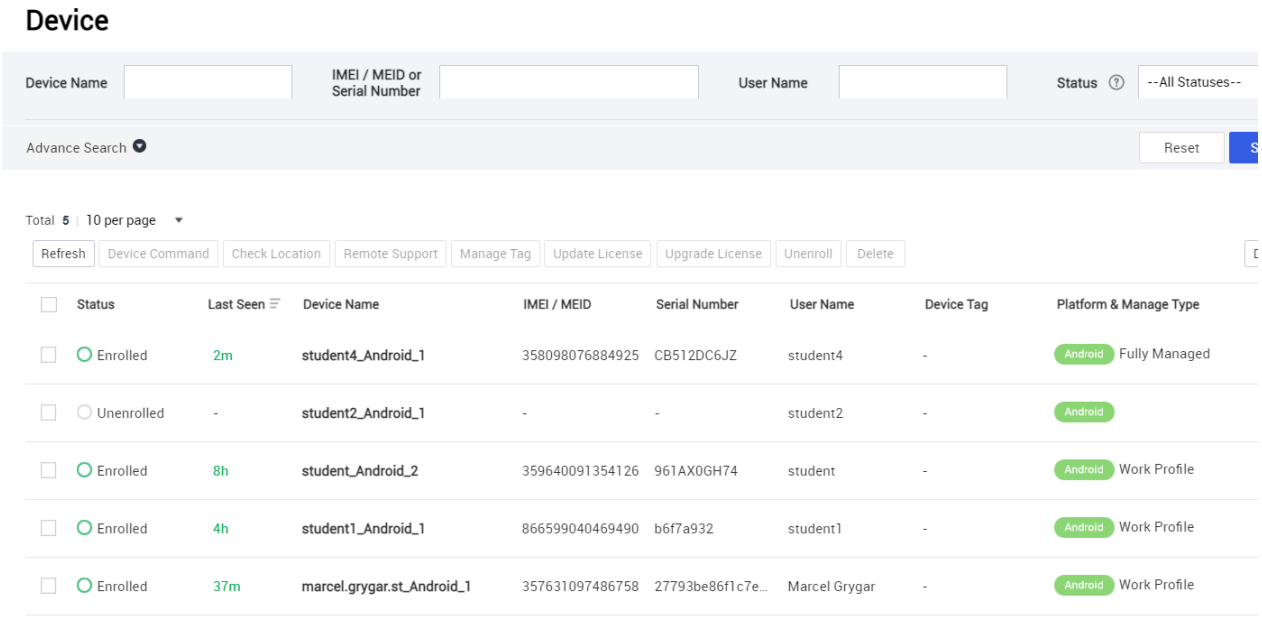
- Po kliknutí na záložku User vidí administrátor seznam všech uživatelů, viz obrázek 4.21. Zde je možné uživatele spravovat a nastavovat jejich politiku.

Group

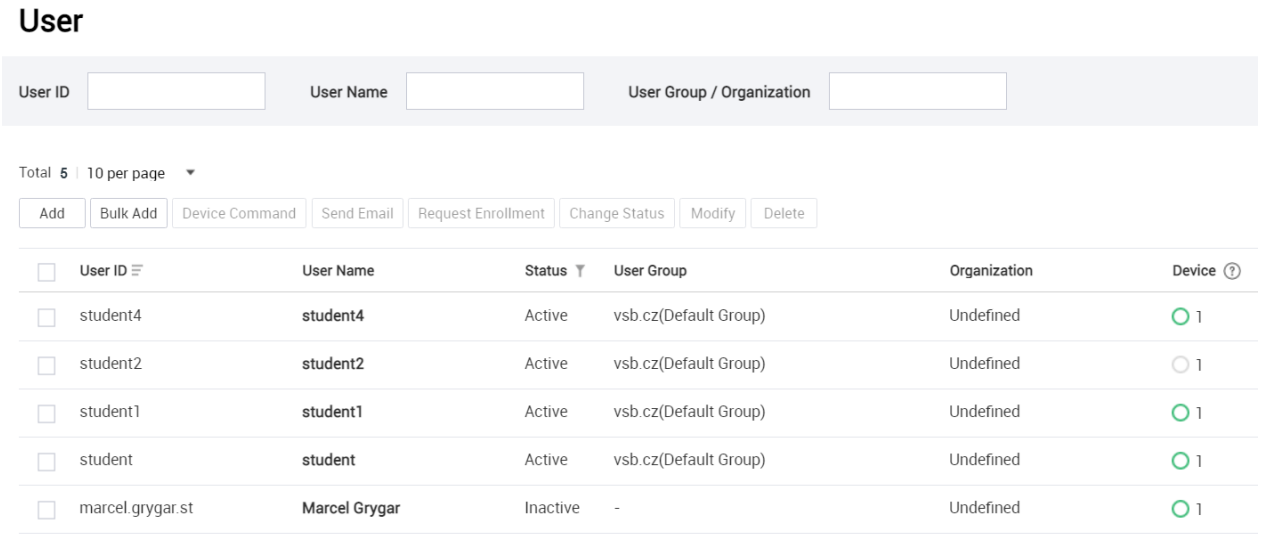
- V záložce Group vidí administrátor všechny skupiny. Může skupiny vytvářet a zasílat na ně příkazy. Skupině je možné přiřazovat politiku, balíčky aplikací nebo balíčky dokumentů, viz obrázek 4.22.

Organization

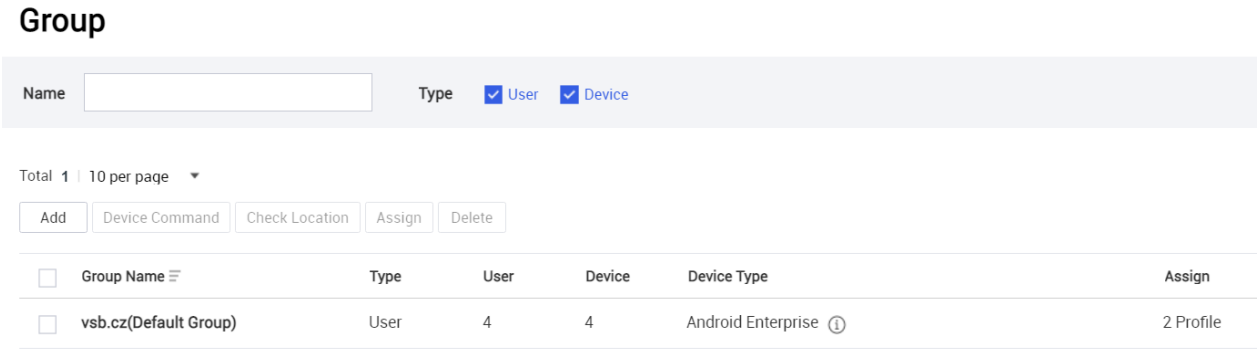
- V této záložce administrátor provádí další úroveň hierarchie nad skupinou, viz obrázek 4.23. Je zde možnost vytvářet podorganizace organizacím, dále zde může přiřazovat celé organizaci politiku, balíčky aplikací a dokumentů. Při vytváření organizace se volí, jestli zařízení, které spadají pod organizaci budou mít pracovní profil nebo ne, také je možnost vytvářet pro organizaci administrátora.



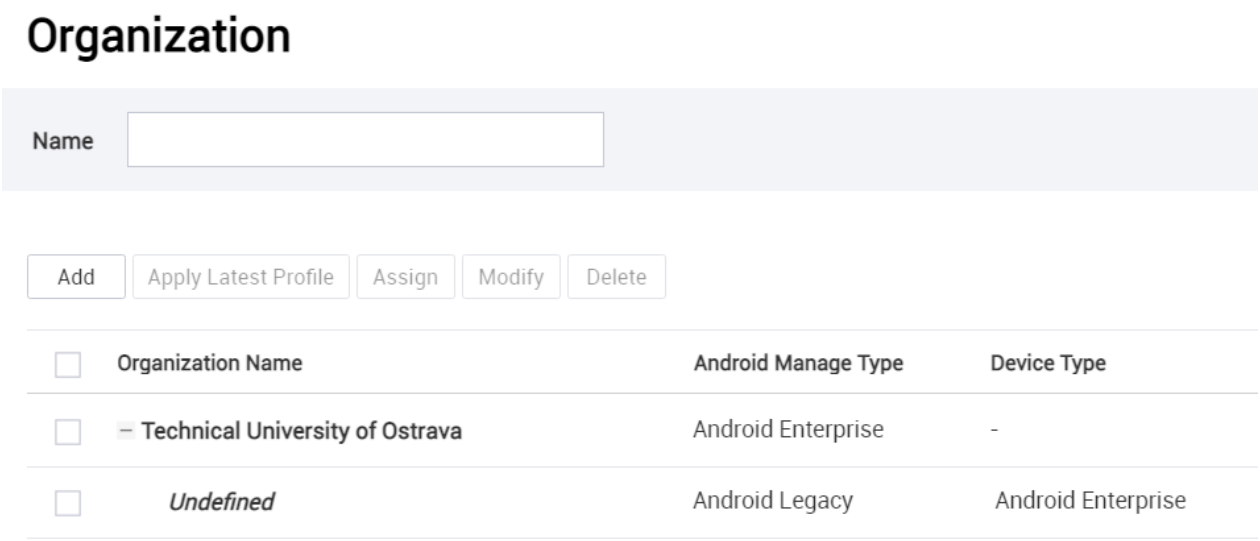
Obrázek 4.20: Samsung Knox Manage Device



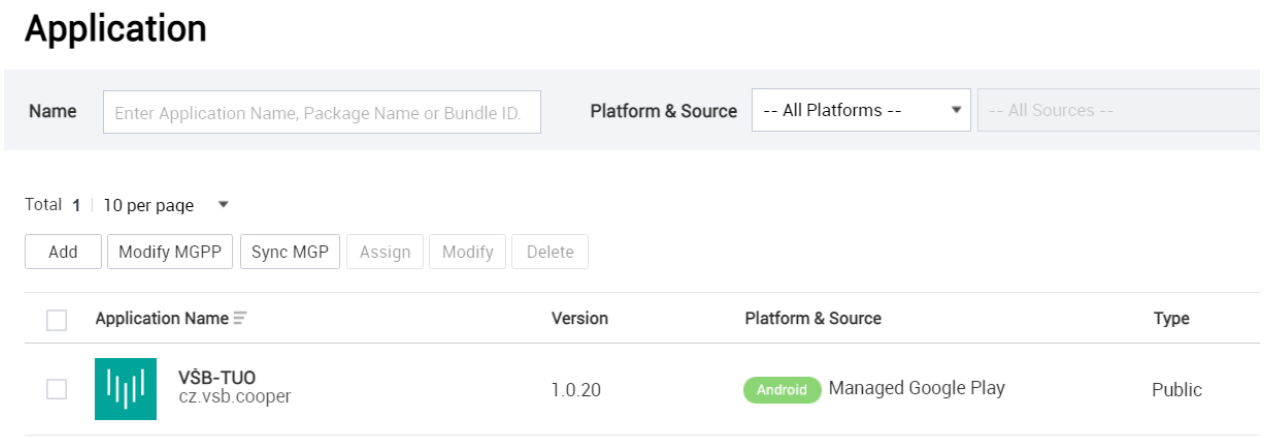
Obrázek 4.21: Samsung Knox Manage User



Obrázek 4.22: Samsung Knox Manage Group



Obrázek 4.23: Samsung Knox Manage Organization



Obrázek 4.24: Samsung Knox Manage Application

Application

- Zde administrátor vidí aplikace, které jsou přidané v podnikovém obchodu a může je odtud spravovat, viz obrázek 4.24.

Profile

- Na záložce Profile může administrátor vytvářet politiky, které následně přiřazuje skupině. Při označení konkretní politiky lze politiku upravit nebo smazat, viz obrázek 4.25.

Kiosk

- V této záložce může administrátor vytvořit Kiosk režim, což je předdefinovaná sada aplikací nebo aplikace, kterou administrátor spouští na zařízeních. Po aktivaci Kiosk režimu budou všechny ostatní aplikace a funkce zařízení deaktivovány, kromě výše zmíněných aplikací, které do zařízení administrátor přidá, viz obrázek 4.26.

Content

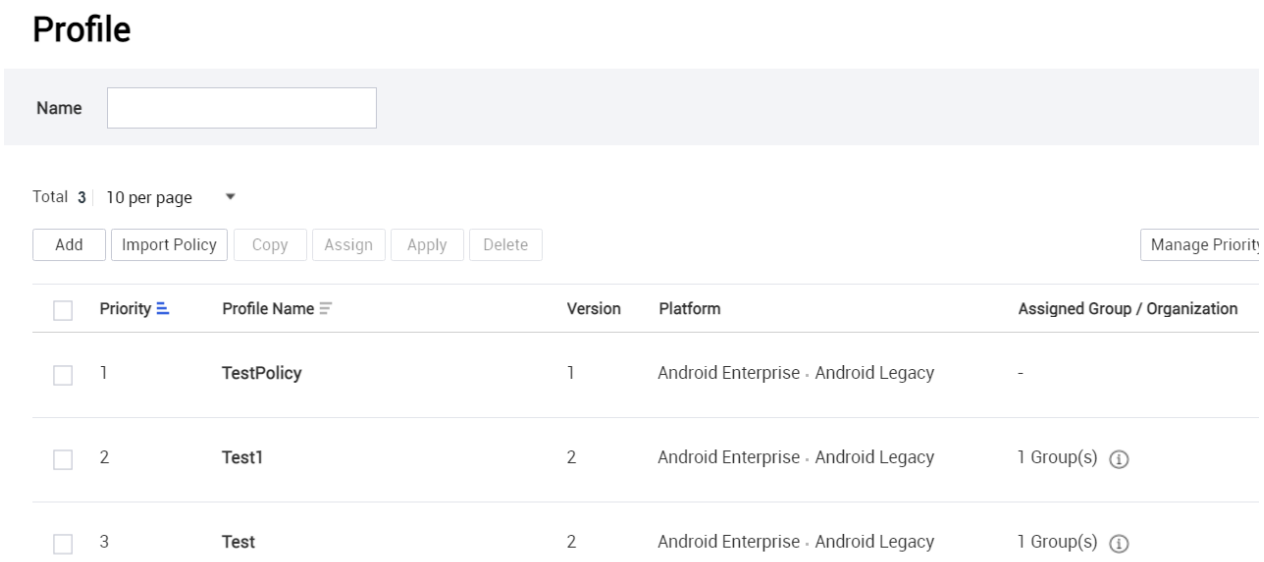
- V tomto rozhraní může administrátor posílat na zařízení dokumenty. Může je přiřadit všem zařízením, určitým skupinám nebo uživatelům či organizacím.

Device Enrollment

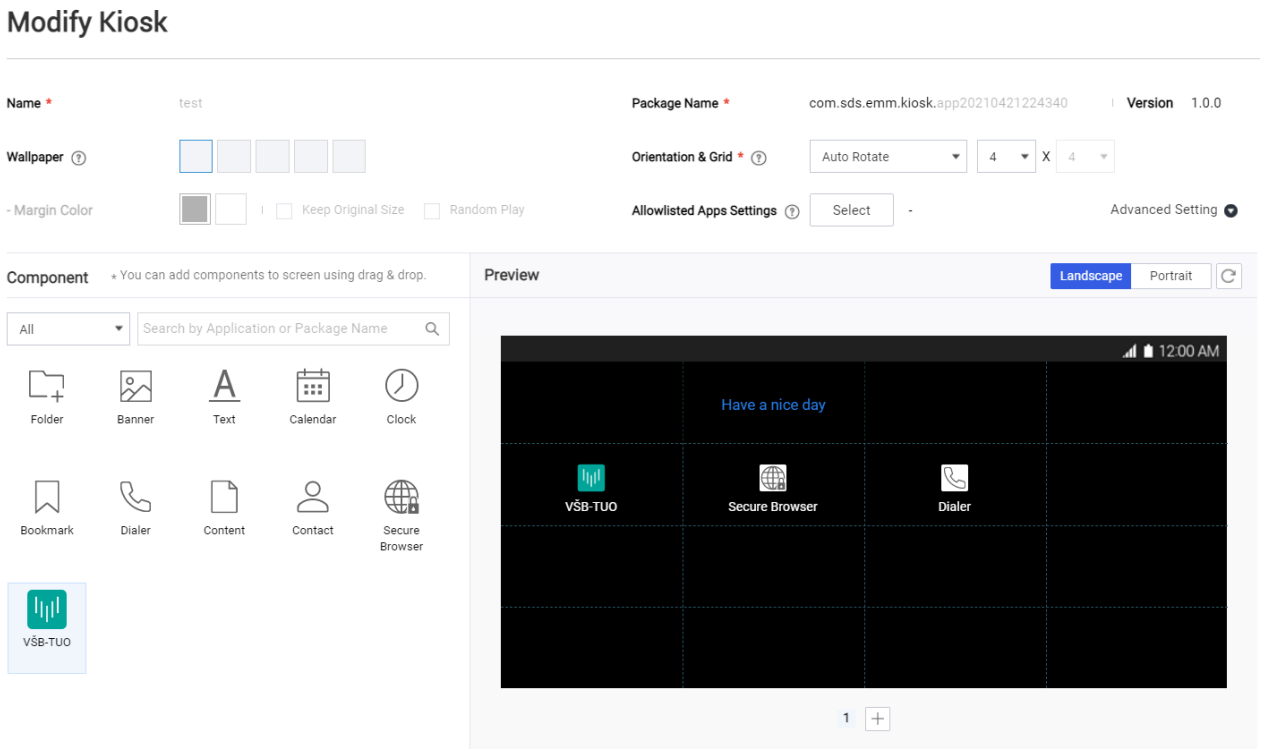
- V tomto rozhraní může administrátor využít možnost zero-touch pro zařízení skrze software Knox Mobile Enrollment.

History

- Zde vidí administrátor záznamy o událostech, jako jsou příkazy pro skupiny nebo zařízení, historii změn a jakoukoliv komunikaci mezi serverem a zařízením.



Obrázek 4.25: Samsung Knox Manage Profile



Obrázek 4.26: Samsung Knox Manage Kiosk

Settings

- V záložce Settings může administrátor upravovat nastavení pro Android a jiné operační systémy, které EMM podporuje. Dále zde může administrátor přidávat další administrátory a přidávat jim práva a také zde může měnit nastavení Android Enterprise.

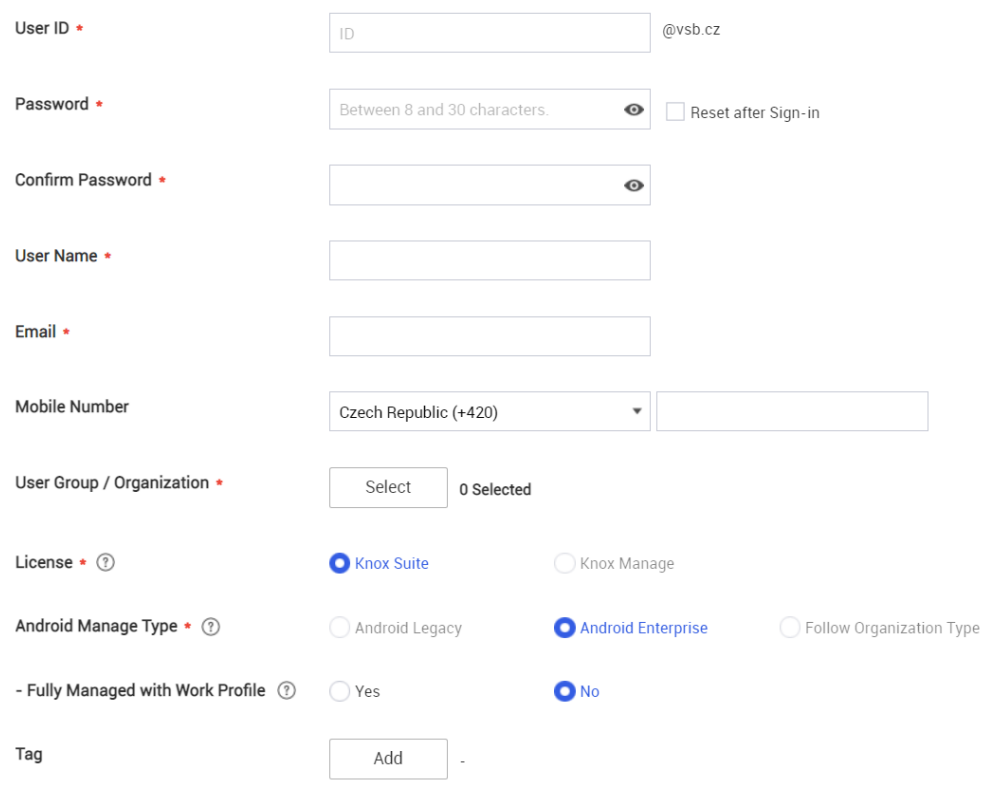
Advanced

- Zde může administrátor nastavovat pokročilejší funkce, jako je synchronizace s Active Directory nebo konfigurace Microsoft Exchange Serveru a využívání jeho funkcí.

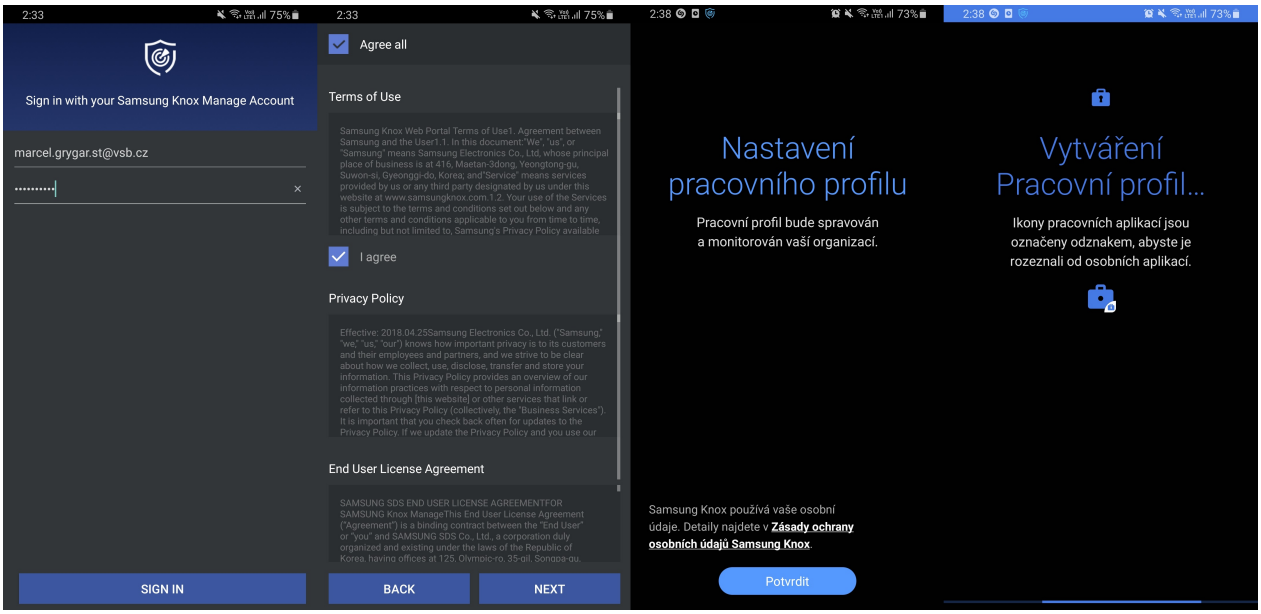
4.2.2 Připojení zařízení k řešení Samsung Knox Manage

Po přihlášení do Samsung Knox Manage administrátora donutí software registrovat EMM přes Google administrátorský účet. Proces je podobný, jako u jiných řešení a jsou zde dvě možnosti, skrze G Suite nebo přes Android Eneteprise Standalone, viz obrázek A.3. Je nutné přidat skupinu nebo organizaci, jelikož bez tohoto nemůže administrátor přidat uživatele. Po přidání skupiny je možné přidat uživatele, viz 4.28. Po obdržení emailu si uživatel stáhne aplikaci, která bude komunikovat se serverem, viz obrázek 4.27. Zadá údaje z emailu při přihlašování k serveru a zaregistruje tím své zařízení, viz obrázek 4.29. Touto registrací si zaměstnanec zaregistruje zařízení Work Profile, pokud bude administrátor chtít zaregistrovat Device Owner zařízení, může tento proces udělat přes aplikaci Knox Enrollment nebo může využít QR kód v emailu. Pro profil Device Owner je nutné zařízení resetovat do továrního nastavení a aktivovat QR skener.

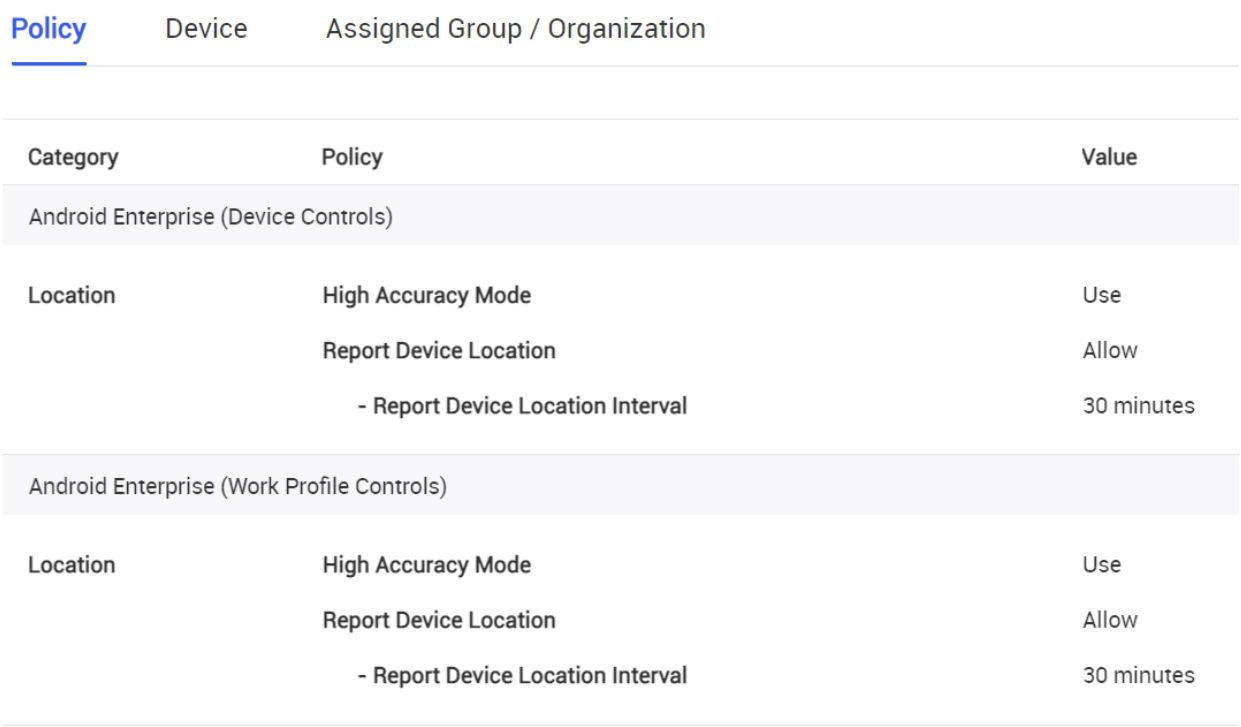
Obrázek 4.27: Samsung Knox Manage email



Obrázek 4.28: Samsung Knox Manage přidání zařízení



Obrázek 4.29: Samsung Knox Manage instalace



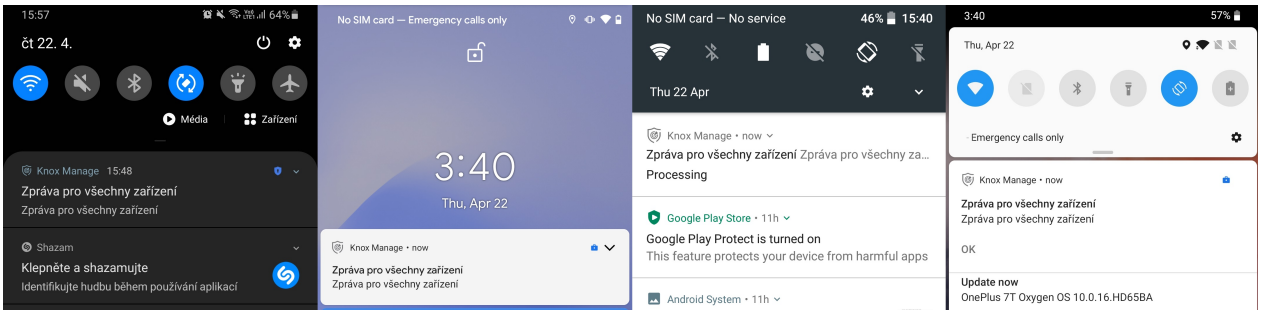
Obrázek 4.30: Samsung Knox Manage politika pro zjištění lokace

4.2.3 Testování funkčnosti Samsung Knox Manage

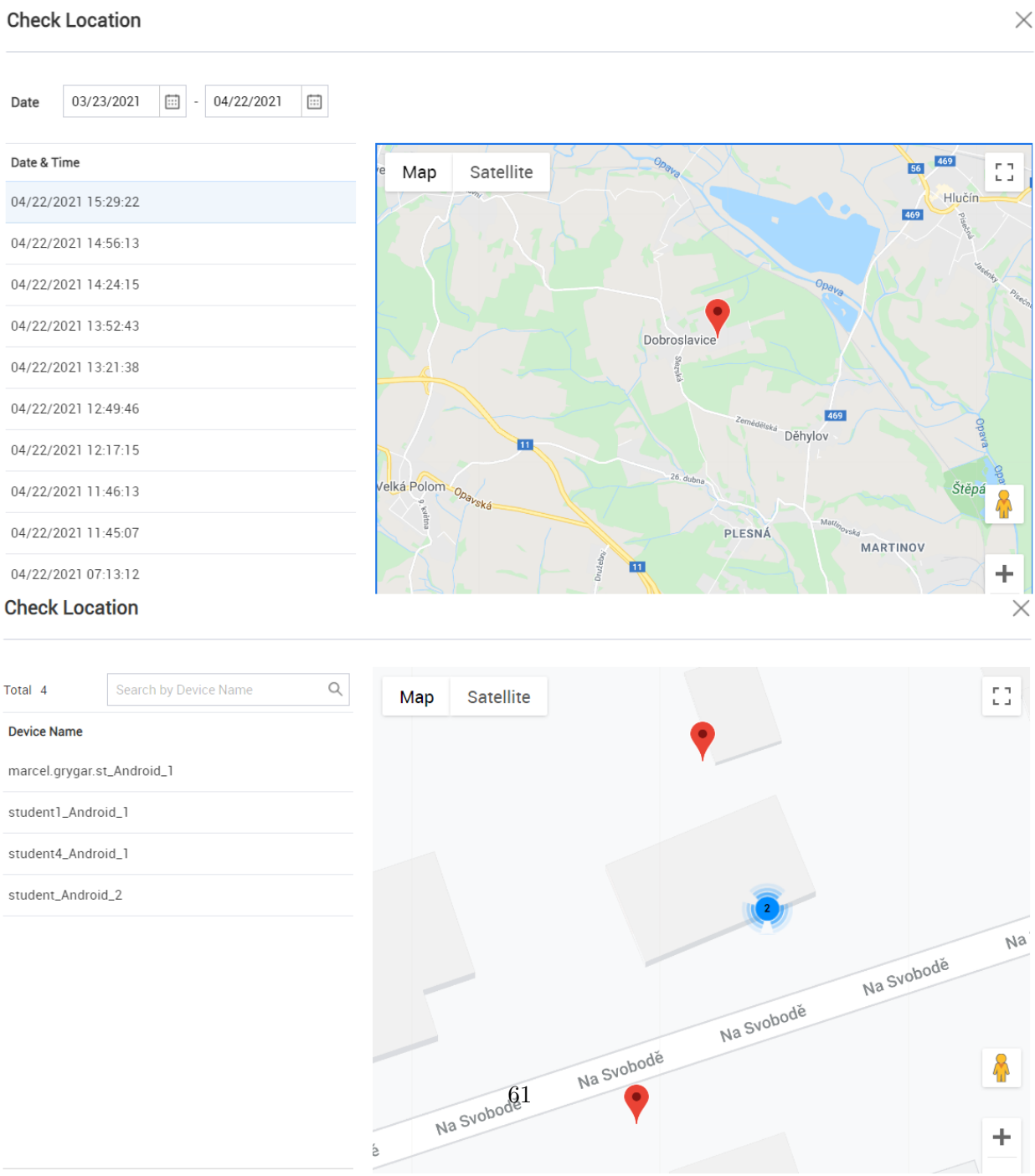
Ze stejných důvodů jako v případě MaaS360 není možné využít zařízení Huawei, viz obrázek A.2.

Testovací scénář je následující. Poslal jsem na zařízení zprávu, poté jsem nastavil Kiosk režim na zařízení. Dále jsem distribuoval aplikace do firemního obchodu, včetně nastavení politiky jak pro Profile Work, tak pro Device Owner zařízení. U politiky jsem nastavil 30 minutový interval na zjištění pozice zařízení a zablokoval jsem použití fotoaparátu u Device Owner zařízení.

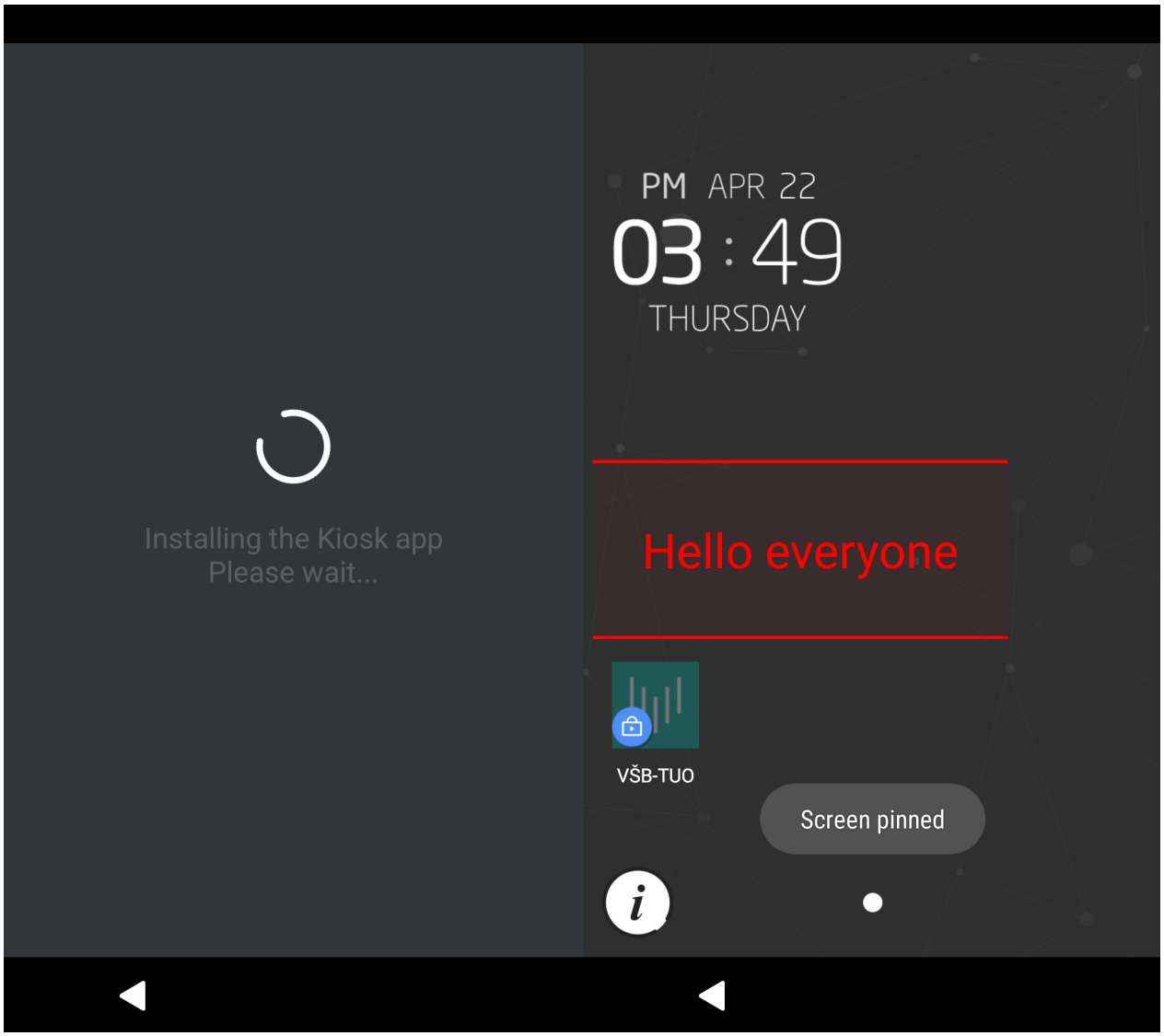
Aby administrátor poslal na zařízení zprávu, musí vstoupit do rozhraní Device, User nebo Group. Po zaškrtnutí boxu může administrátor na zařízení vyslat příkaz, viz obrázek 4.31. Bohužel u Device Owner a Profile Owner zařízení musí akci provést zvlášť, jelikož nemůže na zařízení s různými profily posílat příkaz. Aby administrátor zjistil lokaci zařízení musí nejprve nastavit politiku u zařízení. Pro nastavení politiky musí administrátor jít do záložky Profile a vytvořit novou politiku a následně v ní nastavit zjištění lokace, viz obrázek 4.30. Pro zobrazení lokace musí administrátor přejít do rozhraní Group nebo Device a následně si musí zvolit příkaz Check Location, viz obrázek 4.32. Aby administrátor nastavil Kiosk režim, musí ho prvně vytvořit v rozhraní Kiosk. Zde si zvolí, jak bude Kiosk režim vypadat a následně ho podobně jako u lokace musí přidat do politiky a zaslat na zařízení, viz obrázek 4.33.



Obrázek 4.31: Samsung Knox Manage zprávy na zařízení



Obrázek 4.32: Samsung Knox Manage GPS lokace



Obrázek 4.33: Samsung Knox Manage Kiosk

Testování proběhlo v pořádku, kromě samotné instalace klienta, který komunikuje se serverem. Z nějakého neznámého důvodu nebylo možné nainstalovat na zařízení Sony Xperia X a ONEPLUS 7T aplikaci z Google Play. Řešením bylo stáhnutí APK (Android application package) souboru a následně nainstalování aplikace. Zařízení neměla problém komunikovat se serverem, každopádně z pohledu uživatele může toto vyvolat nedůvěru k samotnému EMM provedení. Nezaznamenal jsem rozdíl mezi správnou Samsung zařízení, oproti ostatním zařízením, které jsem testoval.

4.3 Headwind MDM

V rámci práce bylo nutné vyzkoušet si open source řešení, což byl hlavní důvod, proč jsem si vybral tento software. Headwind MDM lze získat přes oficiální stránky společnosti. Na výběr je možnost jak verze zdarma, tak verze Enterprise. U verze Enterprise není možnost veřejně zažádat o místní řešení, každopádně po emailové komunikaci je možné si tuto verzi vyzkoušet. K instalaci je potřeba veřejná IP adresa, případně doména s veřejnou IP adresou.

4.3.1 Konfigurace MDM serveru Headwind MDM

Preferovaný operační systém pro tento MDM server je Ubuntu Linux. Konfigurace serveru je uskutečněna na tomto operačním systému. Celé řešení je možné nastavit na jakémkoliv operačním systému, jelikož software využívá multiplatformní technologii Java a je zprovozněn na technologii Apache Tomcat.

Po instalaci Ubuntu 18.04 je potřeba nainstalovat potřebný software. Prvně je potřeba aktualizovat dostupné repositáře pro instalaci aktuálních služeb a balíčků.

```
sudo apt update
sudo apt install openjdk-8-jdk aapt tomcat8 postgresql
```

Listing 4.1: Instalace požadováného softwaru

Následně je nutno vytvořit databázi s uživatelem a heslem. Tyto informace je třeba si zapamatovat.

```
sudo su postgres
psql
postgres=# CREATE USER student WITH PASSWORD 'student';
postgres=# CREATE DATABASE hmdm WITH OWNER=hmdm;
```

Listing 4.2: Vytvoření databáze

Instalační skript pro Headwind MDM je možné stáhnout přes webový prohlížeč na oficiální stránce dodavatele. Dále je možné ho získat ze stránky Github. Po rozbalení složky je nutné spustit příkaz.

```
sudo ./hmdm_install.sh
```

Listing 4.3: Spuštění instalačního skriptu

Po spuštění instalačního skriptu se nás bude skript dotazovat na nastavení serveru. V hranatých závorkách je výchozí nastavení. Prvně se skript zeptá na jazyk, ve kterém bude instalace provedena, na výběr je mezi ruským a anglickým jazykem. Následně bude chtít přístup do již vytvořené databáze. Poté je nutné zvolit, kde se server nainstaluje. V dalším kroku je volba protokolu HTTP nebo

HTTPS a naší veřejné IP adresy, případně domény. Důležité je také zvolení portu, na kterém bude služba fungovat. V mém případě jsem postupoval následovně.

```
PostgreSQL database setup
=========================
PostgreSQL host [localhost]: localhost
PostgreSQL port [5432]: 5432
PostgreSQL database [hmdm]: hmdm
PostgreSQL user [hmdm]: student
PostgreSQL password: student

File storage setup
==================
Headwind MDM directory [/opt/hmdm]: /opt/hmdm

Web application setup
=====================
Protocol (http|https) [http]: http
Domain name or public IP (e.g. example.com): grygar.cenyrealit.cz
Port (leave empty for default ports 80 or 443): 8080
Project path on server or ROOT [/hmdm]: /hmdm
Tomcat virtual host [localhost]: localhost
```

Listing 4.4: Nastavení instalačního skriptu

V tuhle chvíli se administrátor může připojit na webové rozhraní, přihlásit se do MDM a začít přidávat zařízení.

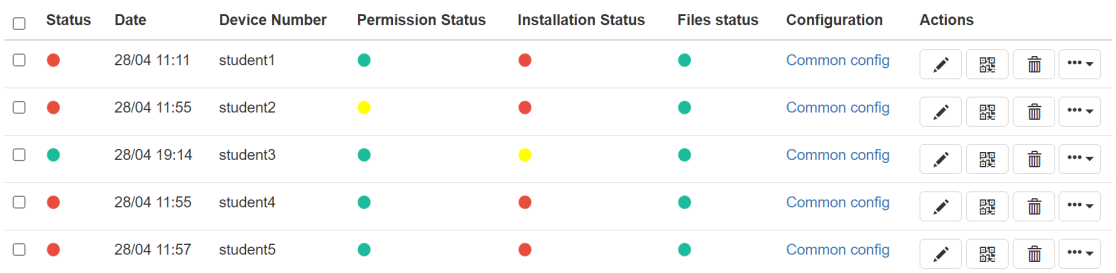
4.3.2 Administrátorské rozhraní Headwind MDM

Na obrázku 4.34 lze vidět co vidí administrátor po přihlášení do Headwind MDM. Navigace se rozděluje na Devices, Applications, Configurations, Files, Settings a Functions.

Obrázek 4.34: Headwind MDM navigace

Device

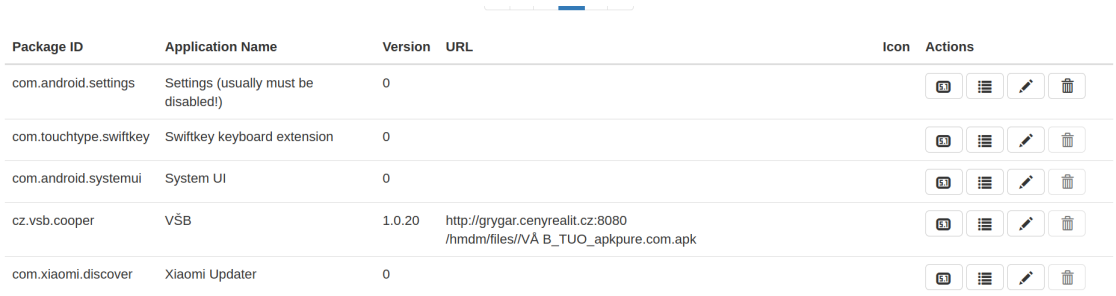
- V tomto rozhraní vidí administrátor všechny zařízení, viz obrázek 4.35. Nejsou zde uživatelé a zařízení se přidávají pod Device Number. Po zaškrtnutí boxu je možné na zařízení posílat příkazy a také je zde možnost přepínat mezi skupinami.



Obrázek 4.35: Headwind MDM Device

Applications

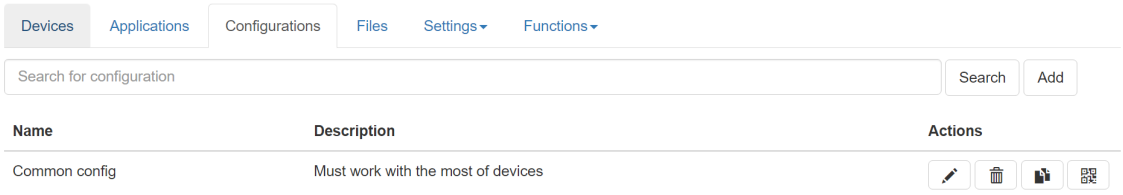
- Zde může administrátor poslat na zařízení aplikaci, viz obrázek 4.36. Jelikož toto řešení nepodporuje Android Enterprise, tak zde není možnost přidat aplikace do zařízení skrze Google Play obchod. Na serveru se ukládají aplikace, které se následně zasílají ze serveru do zařízení. Uložené aplikace mohou být pouze ve formátu APK, neboli soubory s příponou .apk a .xapk.



Obrázek 4.36: Headwind MDM Applications

Configurations

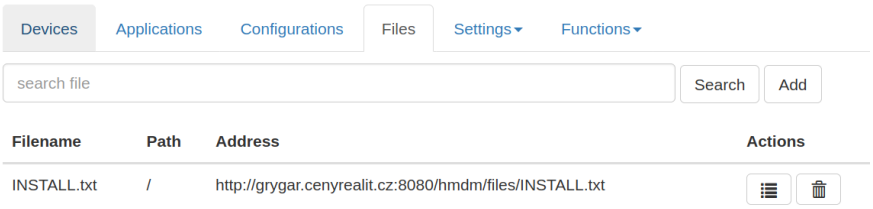
- V této záložce administrátor nastavuje politiky pro zařízení, viz obrázek 4.37. Dále zde může přidávat politiku aplikacím a upravovat, jak bude Kiosk režim vypadat.



Obrázek 4.37: Headwind MDM Configurations

Files

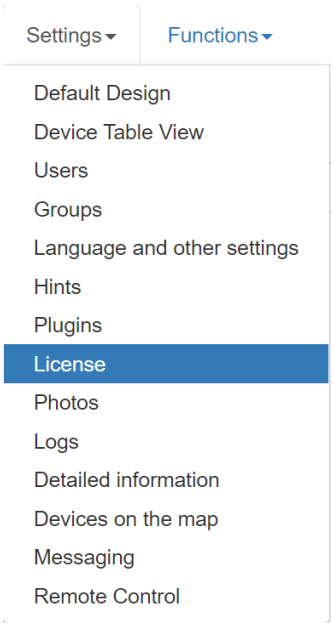
- Pro zasílání souboru na zařízení musí administrátor přejít do záložky Files, odkud může přidat jakýkoliv soubor a zaslat ho na zařízení, viz obrázek 4.38.



Obrázek 4.38: Headwind MDM Files

Settings

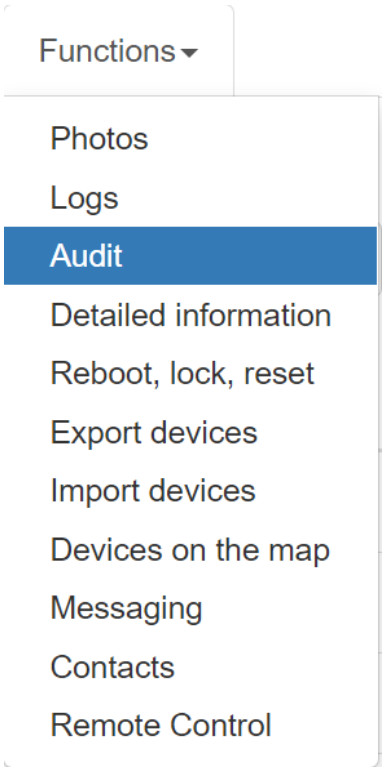
- Pro nastavení MDM serveru a jeho funkcí musí administrátor vstoupit do rozhraní Settings, viz obrázek 4.39. Zde může administrátor zvolit například následující nastavení:
  - přidání dalšího uživatele s právy,
  - přidání skupiny,
  - změnu licence,
  - jak dlouho se zařízení bude ukládat poloha a
  - jak dlouho se budou ukládat záznamy o příkazech.



Obrázek 4.39: Headwind MDM Settings

Functions

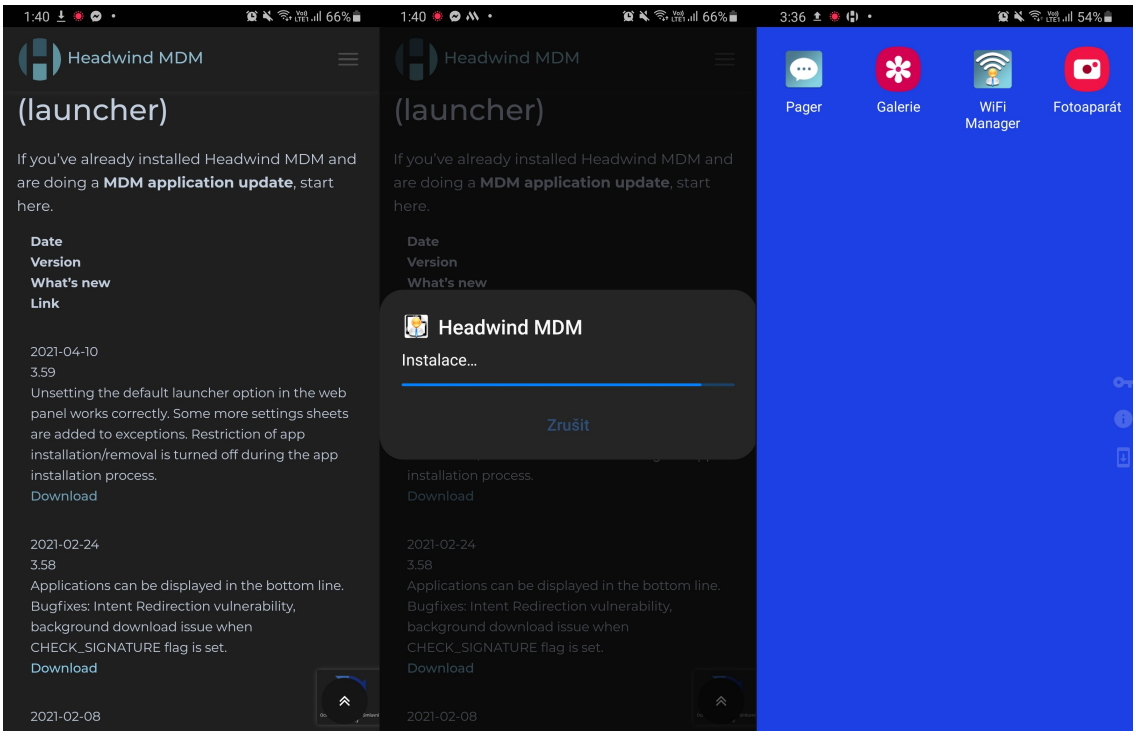
- V tomto rozhraní může administrátor pracovat s různými funkcemi, jako je například:
  - lokace zařízení na mapě,
  - exportování dat ze zařízení v podobě excelu,
  - vzdálená kontrola nad zařízením,
  - zobrazení zpráv které se zaslaly na zařízení a
  - zobrazení záznamu o zařízení, viz obrázek 4.40.



Obrázek 4.40: Headwind MDM Functions

4.3.3 Připojení zařízení k řešení Headwind MDM

Administrátor může zařízení připojit pouze skrze QR kód nebo APK tím, že si vytvoří Device Number a následně si vytvoří QR kód nebo stáhne APK z oficiálních stránek společnosti. Zařízení je nutno uvést do továrního nastavení a následně povolit QR kód tím, že se několikrát administrátor nebo zaměstnanec dotkne displeje. Zařízení je uvedeno do Kiosk režimu, jakmile se zaregistruje a následně jsou na něj nainstalované aplikace, viz obrázek 4.41. Z Kiosk prostředí se lze zpátky přesunout do Android prostředí, ale je možné to uživateli znemožnit. Při instalaci bude Headwind MDM vyžadovat adresu serveru a Device Number, pod který se přiřadí.



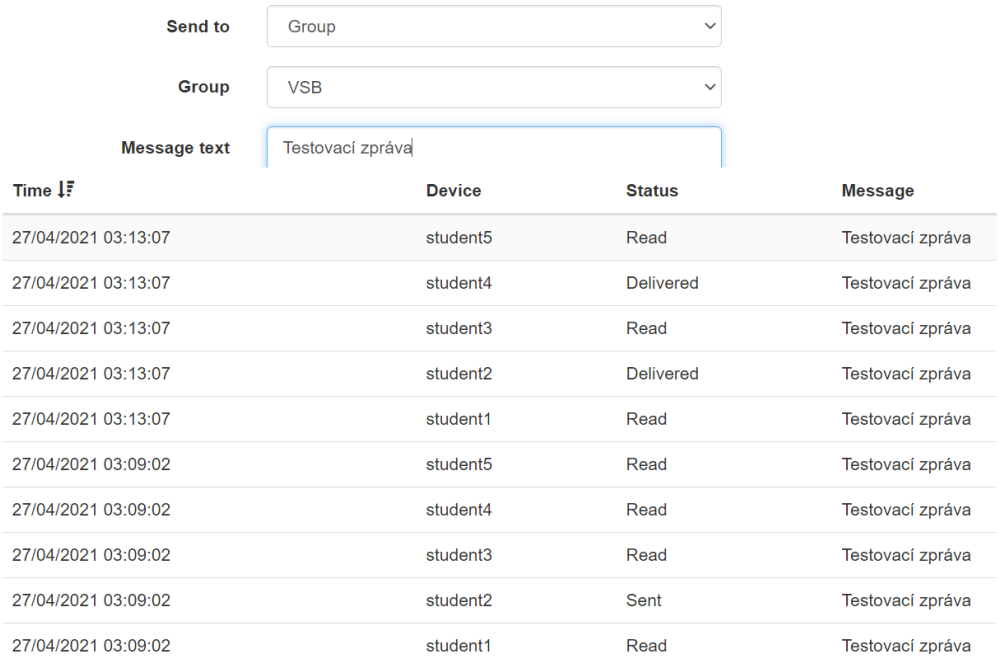
Obrázek 4.41: Headwind MDM přidání zařízení

4.3.4 Testování funkčnosti Headwind MDM

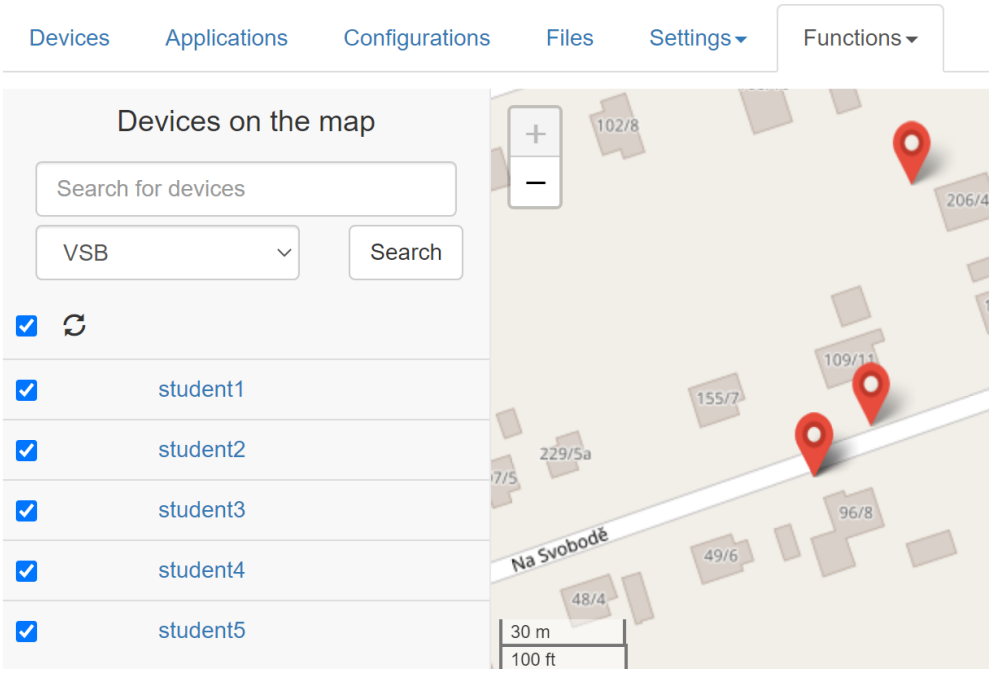
Kvůli absenci QR skeneru po resetování zařízení, nebylo možné využít tuto metodu pro přidání Huawei zařízení do správy a bylo nutné stahovat APK balíček.

Testovací scénář bude následující, pošlu na zařízení zprávu a následně si zobrazím lokaci zařízení. Pošlu na zařízení aplikaci a soubor. Na zařízeních není nastaveno heslo, takže zaměstnancům vynutím heslo pomocí politiky.

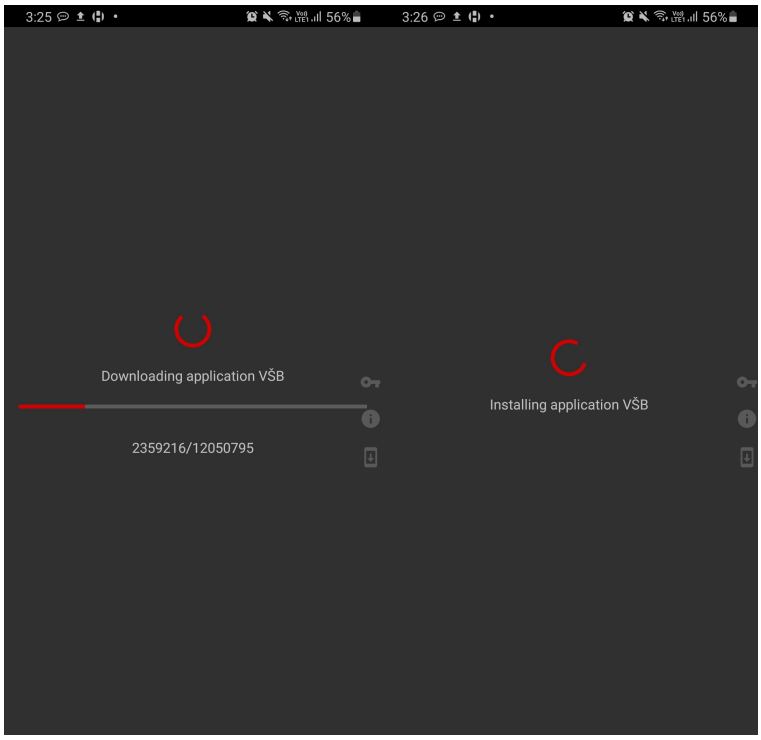
Pro zaslání zpráv na zařízení musí administrátor přejít buď do rozhraní Devices nebo Functions. Po vybrání Device Number může administrátor na zařízení zaslat zprávy, viz obrázek 4.42. Pro zobrazení lokace zařízení musí administrátor kliknout na záložku Functions a následně kliknout na tlačítko Devices on the map a zde může filtrovat, která zařízení zrovna na mapě uvidí, viz obrázek 4.43. Co se týče aplikace, tak je nutno vlastnit APK soubor, ten je možné najít v rámci různých stránek, které dokáží z obchodu Google Play tyto APK soubory stáhnout. Následně po stažení má administrátor možnost tyto APK soubory nahrát na server a ze serveru je zaslat na zařízení a nainstalovat. Pokud bude chtít administrátor nahrát soubor, musí jej prvně nahrát na server a následně poslat na zařízení, viz obrázek 4.44. Pro přidání politiky musí administrátor přejít do rozhraní Configurations a zde politiku přidat a následně v politice vynutit zaměstnanci silnější heslo, viz obrázek 4.45.



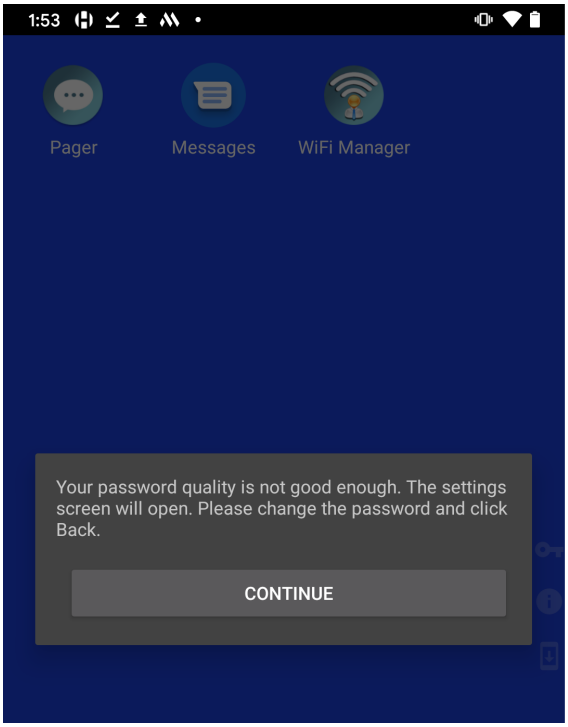
Obrázek 4.42: Headwind MDM zaslaní zpráv na zařízení



Obrázek 4.43: Headwind MDM zobrazení lokace



Obrázek 4.44: Headwind MDM přidání aplikace



Obrázek 4.45: Headwind MDM donucení uživatele změnit heslo

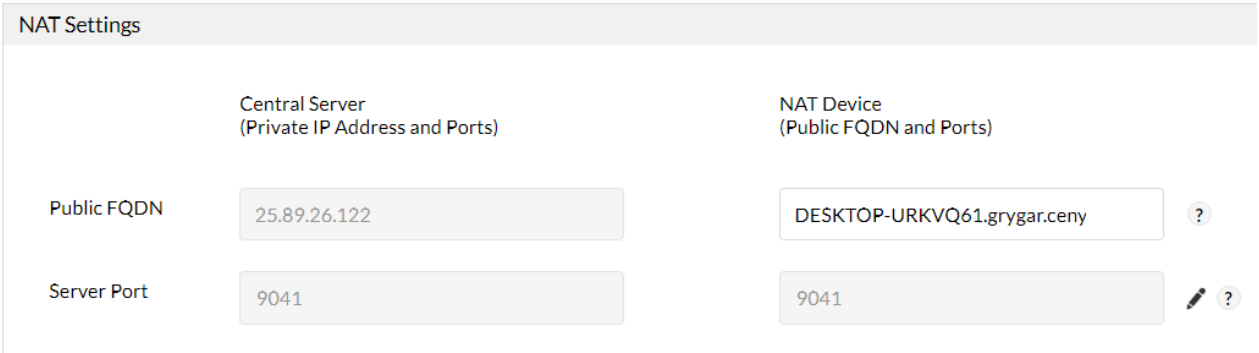
Testování proběhlo bez problému, tentokrát bylo otestováno všech pět mobilních zařízení. Při vyzkoušení odeslání zpráv na zařízení se poprvé vyskytla chyba u zařízení od společnosti Sony, každopádně druhá zpráva se na zařízení dostala.

4.4 ManageEngine MDM

ManageEngine MDM je možné získat na oficiálních stránkách společnosti jak ve verzi cloudové, tak ve verzi místní. Důvodem zvolení tohoto řešení je možnost mít řešení zdarma pro 25 zařízení, což je vhodné pro menší firmy. Opět je nutné mít firemní email pro registraci.

4.4.1 Konfigurace MDM serveru ManageEngine MDM

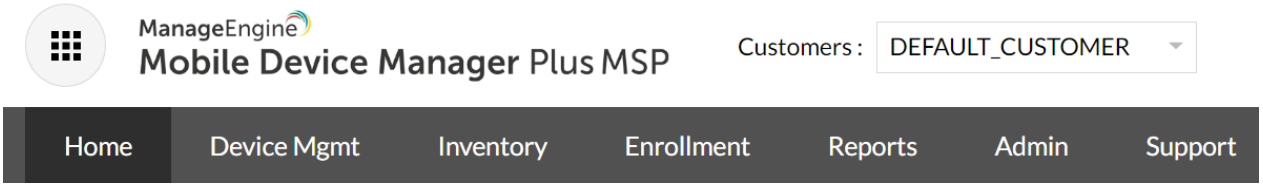
Server je nainstalovaný na desktopovou verzi Windows 10, každopádně firma ManageEngine doporučuje při více jak 1000 zařízeních, využít verzi serverovou. Po stažení instalačního souboru z oficiálních stránek a nainstalování, se automaticky spustí MDM server. Administrátor může zvolit několik možností, jak server nakonfigurovat. Může ho nechat uzavřený v místní síti nebo ho vystavit internetu pomocí překladu síťových adres. Nadále může administrátor zvolit, jestli chce zařízení přidávat přes email, tím pádem bude nutné nastavit emailový server. Následně může administrátor nastavit záložní databázi a server, kdyby nastaly technické potíže s hlavním serverem. V mém případě jsem server připojil k FQDN (Fully Qualified Domain Name) a je možné se na server vzdáleně připojit. Server je zprovozněn na portu 9040 a pro komunikaci používá port 9041, viz obrázek 4.46.



Obrázek 4.46: ManageEngine MDM nastavení serveru pro vnější komunikaci

4.4.2 Administrátorské rozhraní ManageEngine MDM

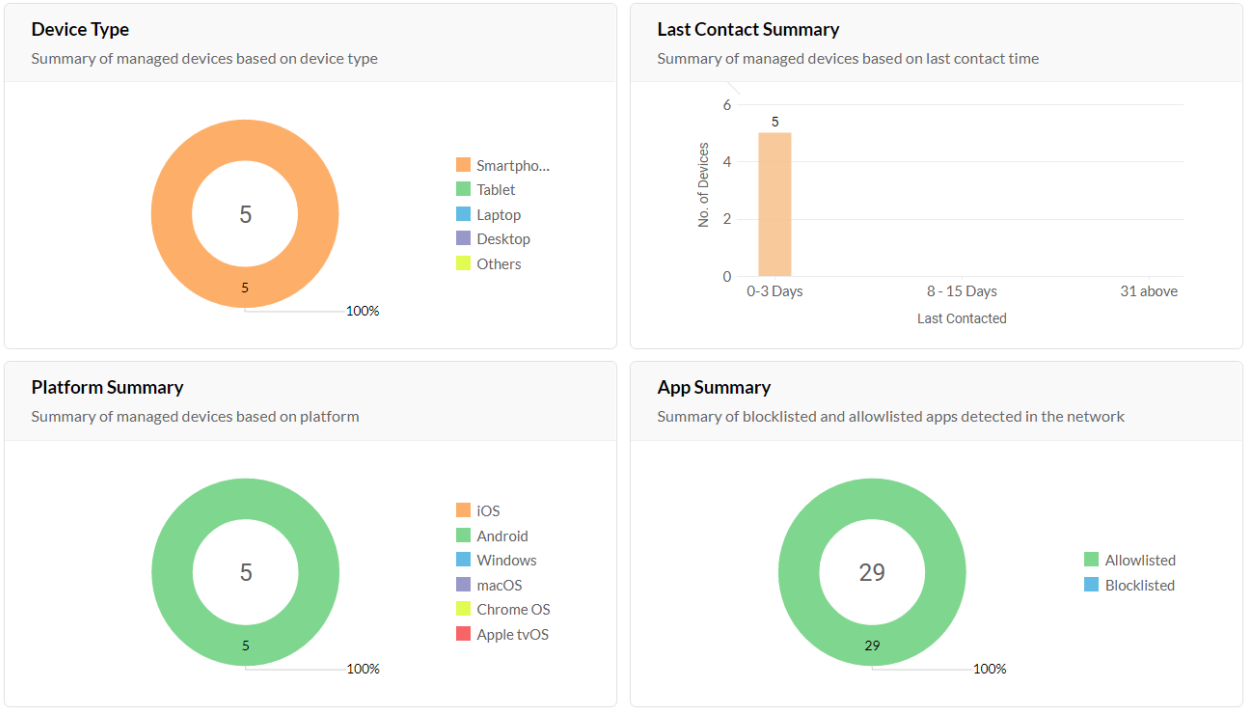
Po přihlášeni do ManageEngine MDM, vidí administrátor vodorovnou navigaci, viz obrázek 4.47.



Obrázek 4.47: ManageEngine MDM navigace

Home

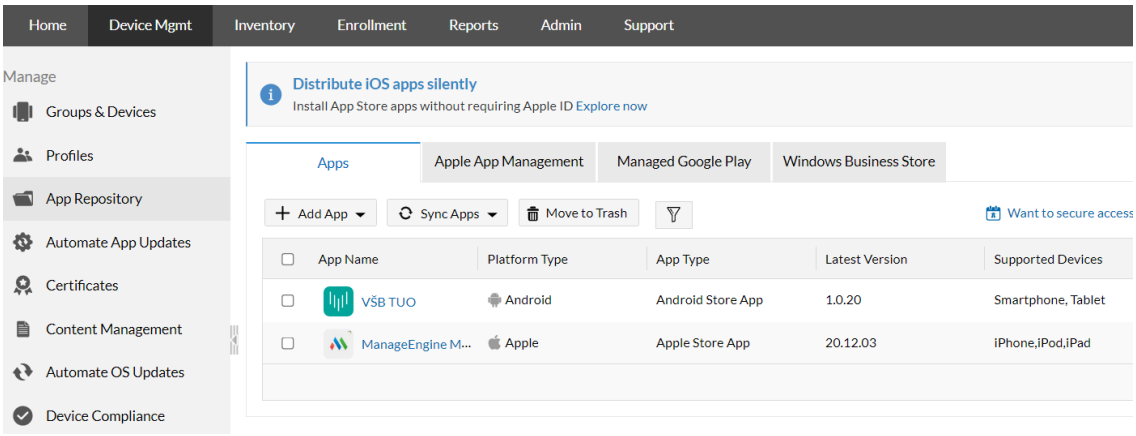
- V tomto rozhraní vidí administrátor přehled o všech zařízeních, jaký je jejich operační systém, souhrn povolených a zakázaných aplikací, shrnutí posledních příkazů na zařízení, kolik zařízení bylo přidáno, kolik uživatelů má přidáno zařízení a kolik zařízení čeká na přidání, viz obrázek 4.48.



Obrázek 4.48: ManageEngine MDM Home

Device Mgmt

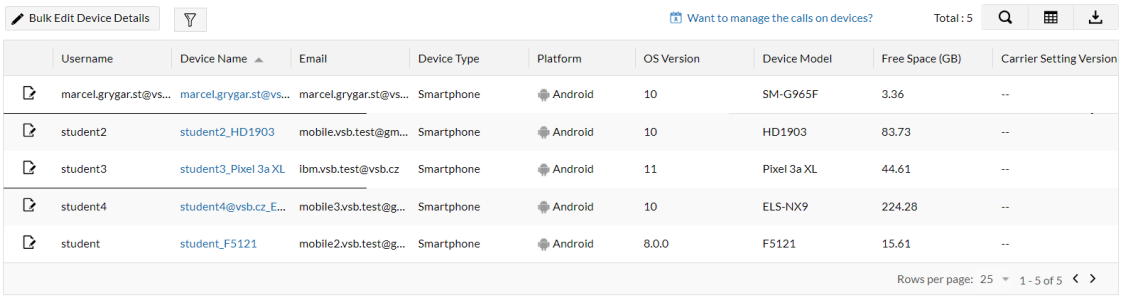
- Zde administrátor vytváří skupiny a uživatele, přidává aplikace do firemního obchodu a přidává na server dokumenty, viz obrázek 4.49. Dále je možné software propojit s Office 365 a Exchange Serverem. Také se zde nastavuje politika pro zařízení.



Obrázek 4.49: ManageEngine MDM Device Mgmt

Inventory

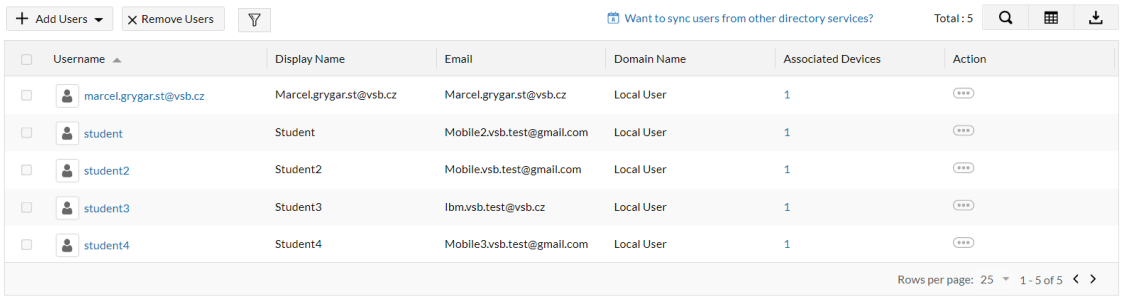
- Pokud bude chtít administrátor zakazovat různé aplikace nebo je povolovat, bude muset přejít do rozhraní Inventory, viz obrázek 4.50. V tomto rozhraní je také možnost zařízením nastavit sledování.



Obrázek 4.50: ManageEngine MDM Inventory

Enrollment

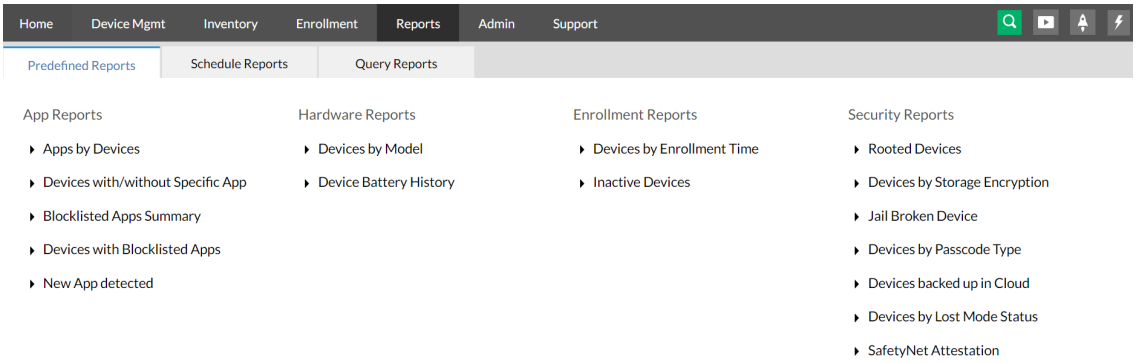
- Pro přidání zařízení musí administrátor přejít do rozhraní Enrollment. Může zde přidávat uživatele a zařízení, viz obrázek 4.51.



Obrázek 4.51: ManageEngine MDM Enrollment

Reports

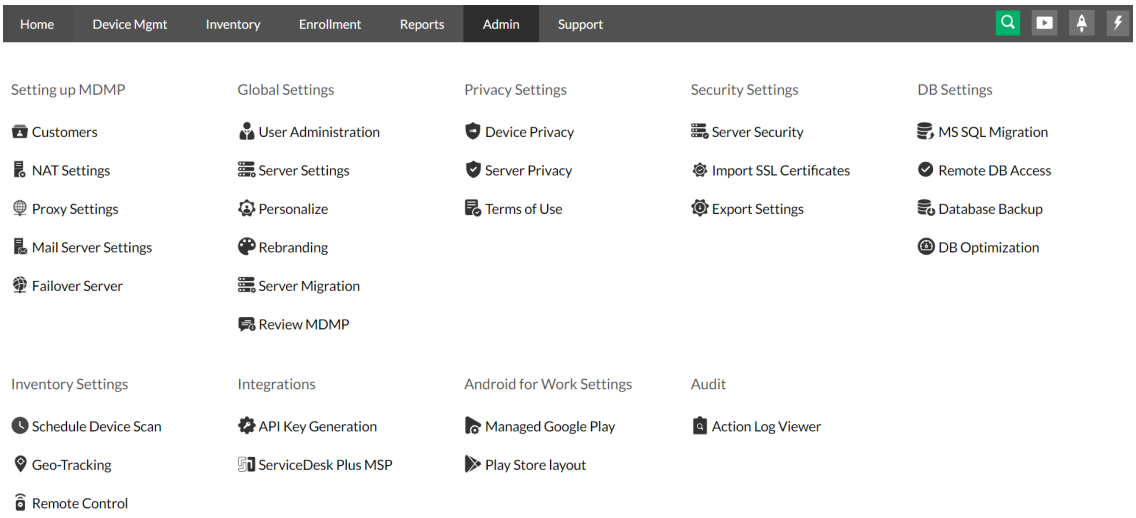
- Jestliže bude chtít administrátor přehled zpráv, seřazovat zařízení podle modelu nebo zobrazit zařízení, které mají narušenou bezpečnost, najde tyto zprávy zde, viz obrázek 4.52.



Obrázek 4.52: ManageEngine MDM Reports

Admin

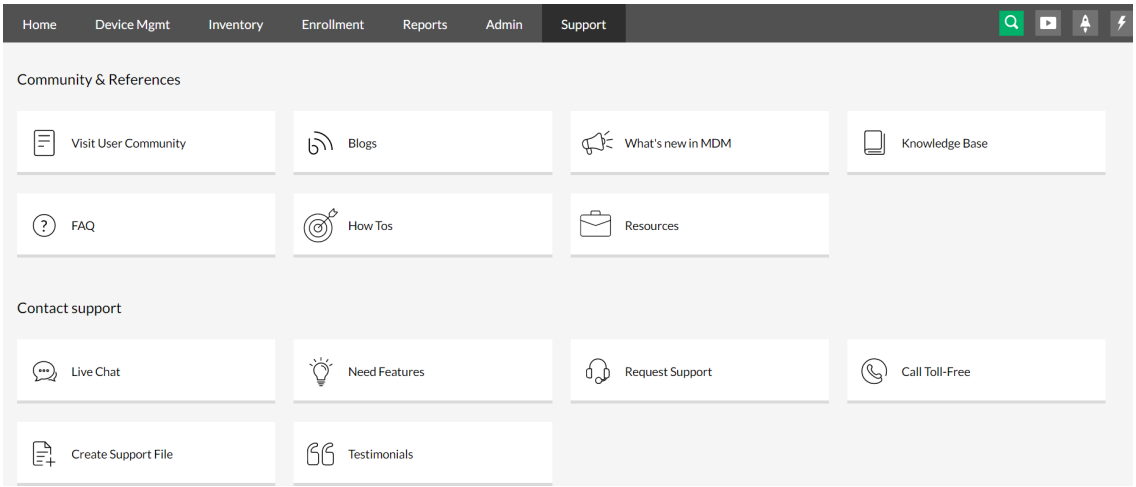
- Administrátor v tomto rozhraní nastavuje všechny možnosti MDM serveru, viz obrázek 4.53. Přidává další administrátory, nastavuje síť, nastavuje zálohu serveru, přidává bezpečnostní certifikáty nebo nastavuje firemní obchod.



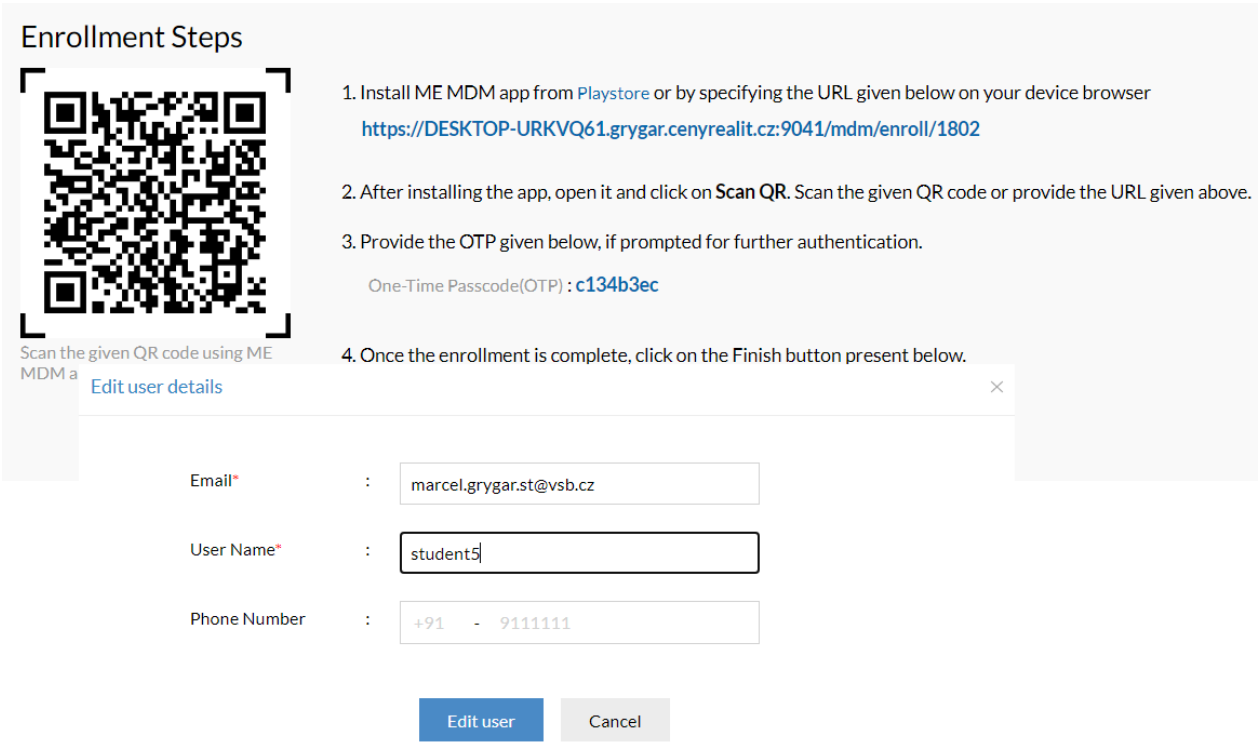
Obrázek 4.53: ManageEngine MDM Admin

Support

- Zde může administrátor najít všechnu dokumentaci, live chat s podporou, vytvořit tiket pro podporu nebo prohledat komunitní fórum, viz obrázek 4.54.



Obrázek 4.54: ManageEngine MDM Support

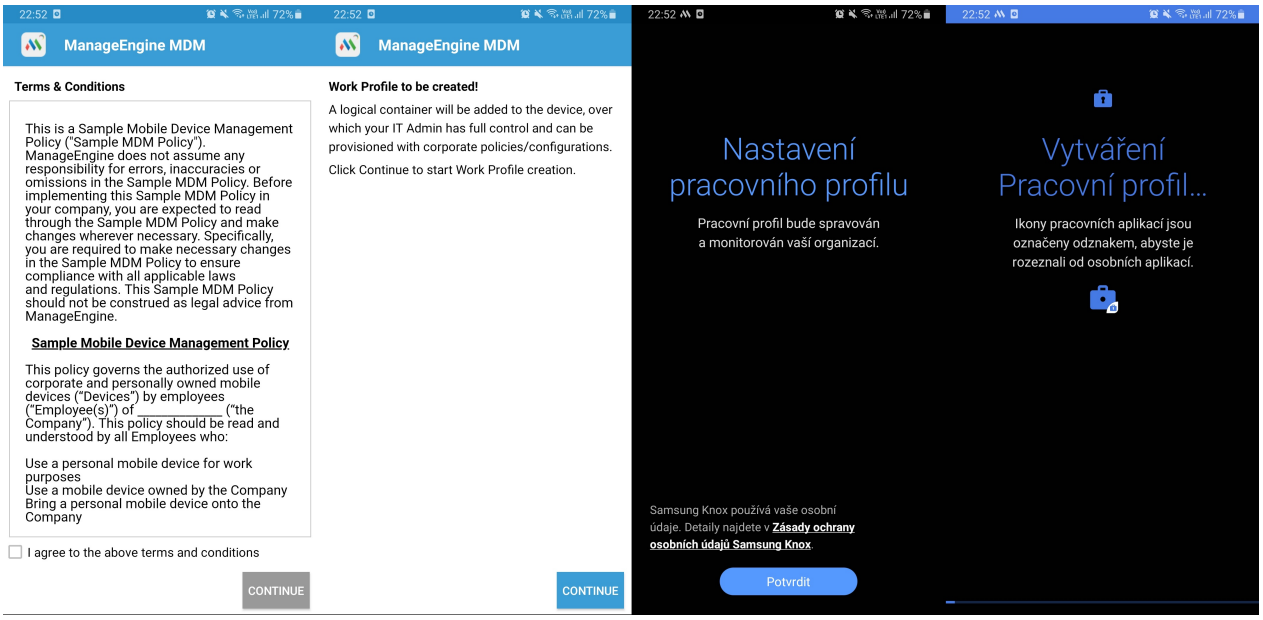


Obrázek 4.55: ManageEngine MDM přidání zařízení

4.4.3 Připojení zařízení k řešení ManageEngine MDM

Jako u softwarů IBM a Samsung jsou zde stejné možnosti pro přidání zařízení. Tentokrát není nutné zařízení registrovat přes Google administrátorský účet, až když administrátor bude přidávat aplikace do Google Play obchodu, viz obrázek A.3. Na výběr má administrátor opět mezi možnostmi Device Owner nebo Profile Work, k tomu se ManageEngine ptá, jestli je zařízení od společnosti Samsung nebo není. V případě, že zařízení je od společnosti Samsung, můžeme pro přidání zařízení použít Knox Mobile Enrollment.

Pro připojení zařízení musí administrátor kliknout na záložku Enrollment a zvolit si Android Devices. Jakmile administrátor zvolí, jestli zařízení je od společnosti Samsung nebo ne, tak se vygeneruje QR kód, viz obrázek 4.55. Zaměstnanec si bude muset stáhnout aplikaci ManageEngine MDM a následně kód naskenovat. Jakmile všechno potvrdí, začne se mu vytvářet profil, viz obrázek 4.56.



Obrázek 4.56: ManageEngine MDM instalace aplikace

4.4.4 Testování funkčnosti ManageEngine MDM

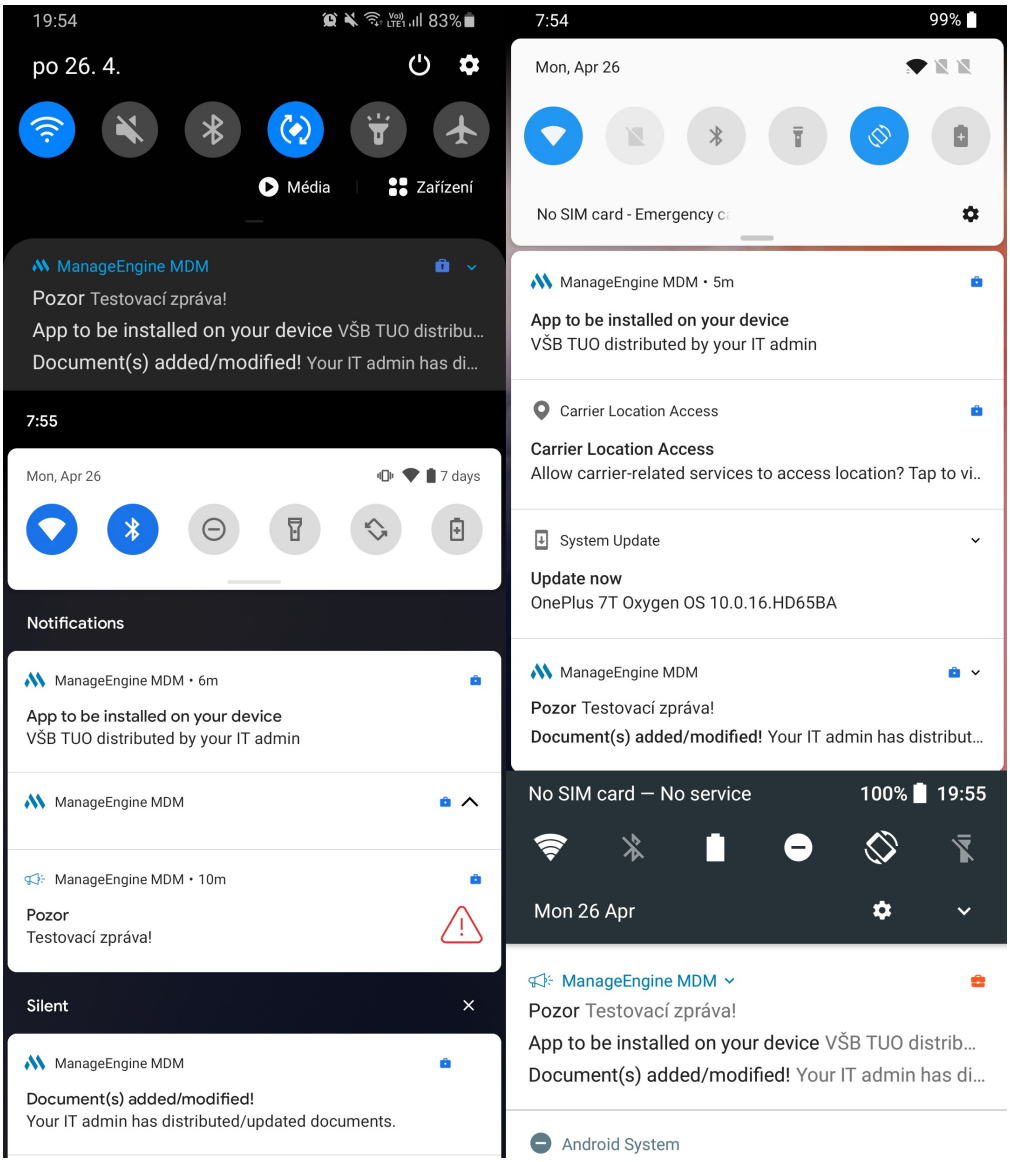
Zařízení Huawei bylo možné do řešení MDM přidat, ale některé funkce nefungovaly.

Testování proběhlo následovně, na zařízení jsem poslal zprávy, následně na zařízení byl ze serveru zaslán dokument a aplikace, a poté jsem na zařízení nastavil politiku.

Aby administrátor poslal zprávu, musí přejít do rozhraní Device Mgmt a zde kliknout na Announcements. Po vytvoření zprávy je možné na skupinu zprávu odeslat. V tomto rozhraní může administrátor poslat aplikaci do firemního obchodu a dokument do zařízení. Pro zaslání aplikací administrátor zvolí App Repository a přidá do obchodu aplikaci. Přes Content Management může zase poslat do zařízení dokument. Zprávu, aplikaci a dokument lze vidět na obrázku 4.57. Pokud bude administrátor chtít vytvořit politiku, bude muset kliknout na Profile a přiřadit ji skupině.

Testování proběhlo na zařízeních bez problému, kromě zařízení Huawei. U zařízení Huawei nebylo možné nainstalovat aplikaci, kvůli absence Google Play, také zde nebylo možné zaslat zprávu na zařízení. Politika se nepřiřadila k zařízení. Jediná funkce, která fungovala byla zaslání souboru na zařízení.

U zařízení Huawei nebylo možné vytvořit firemní obchod a nebylo možné zasílat na zařízení aplikace. Zprávy nebylo možné na Huawei zařízení zaslat, ale dokumenty ano. U ostatních zařízení nebyl problém s žádnou funkcí, která byla testována. Díky tomu, že ManageEngine nenutil vytváření firemního obchodu Google Play při připojení k MDM serveru, tak se zařízení Huawei dokázalo připojit. U softwaru Samsung Knox Manage a IBM MaaS360 se firemní obchod tvořil již během registrování zařízení a tím pádem bylo nutné komunikovat přes GMS službu, kterou ale Huawei zařízení postrádá.



Obrázek 4.57: ManageEngine MDM testování funkcí

Kapitola 5

Závěr

Cílem práce bylo představit možnosti pro správu mobilních zařízení a následně ukázat jejich funkce. Prvním cílem bylo popsání správy mobilních zařízení, co to je mobilní zařízení, a jaké jsou funkce pro spravované zařízení. Následně byly analyzovány výhody a nevýhody z pohledu zaměstnavatele, a jaký je rozdíl mezi MDM, EMM a UEM včetně jejich historie. Také je zde rešerše šesti programů, cenová tabulka a přehled funkcí pro daný software. Tento teoretický popis je součástí druhé kapitoly.

Dále práce poskytuje přehled o platformě Android, a jak je tento operační systém spjatý se správou mobilních zařízení. Bakalářská práce obsahuje přehled architektury, a jak fungují různé metody pro hromadné přidání Android zařízení. V poslední řadě zde najde zaměstnavatel otázky, které by si měl položit, pokud bude nasazovat do firemní struktury správu mobilních zařízení pro operační systém Android.

V rámci praktické práce bylo cílem vytvořit návod, jak zařízení připojit k řešení a následně tyto zařízení otestovat. Součástí návodu byl také popis rozhraní a popis konfigurace MDM serveru. V průběhu připojování zařízení k programům se objevily problémy se zařízením Huawei, jelikož tomuto zařízení už přes rok chybí služba Google Mobile Services. Podobný scénář by byl u novějších zařízeních Honor, které taktéž nemají službu Google Mobile Services. Většina nových zařízení Huawei se u softwarů pro správu MDM stávají nepoužitelné, pokud se do zařízení nenahraje služba Google Mobile Services. Dalším problém se zařízením Huawei byla absence aplikace pro skenování QR kódu při resetování zařízení, v tu chvíli nebylo možné přidat zařízení do Device Owner profilu.

Nejodlišnější ze všech testovaných programů byl program Headwind MDM. Lišil se způsobem přidání zařízení na MDM server. Nebyla zde možnost využít Android Enterprise, se tedy na zařízení nevyužíval firemní obchod Google Play, ani se zde nevytvořil pracovní profil. Zařízení si vytvořila svá vlastní Kiosk prostředí a v tomto prostředí následně probíhá komunikace s MDM serverem. Samsung Knox Manage se lišil tím, že nijak nezachytával zprávy ve svém prostředí. Takhle nebylo možné podívat se na historii zpráv jako u ostatních řešení. Zpráva se objevila pouze jako notifikace. Opět bych zmínil, že u dvou zařízení byl problém s instalací aplikace, která komunikovala s MDM serverem. Po instalaci APK balíčku nebyl problém s přidáním do MDM serveru a testova-

nými funkcemi. ManageEngine byl specifický tím, že stejně jako Headwind MDM nezasílal na email zaměstnanců oznámení, že jejich zařízení bylo přidáno pod správy MDM. U řešení IBM MaaS360 a Samsung Knox Manage se na email zaměstnanců zasílaly všechny informace k přihlášení, včetně QR kódu. Administrátor tedy nemusel zařízení registrovat a uživatel se mohl registrovat sám. U ManageEngine naopak musí administrátor zaslat uživateli vygenerovanou URL stránku nebo QR kód, jelikož se tento proces neprovede automaticky. Toto neplatí pokud je zařízení registrováno pomocí metody Zero-touch enrollment. IBM MaaS360 se lišil hlavně potvrzováním hesla u jakéhokoliv vyslaného příkazu na zařízení. Na druhou stranu zasílání příkazu na zařízení bylo velice jednoduché, nebylo nutné příkaz potvrzovat přes politiku nebo hierarchii skupin jako u řešení Samsung Knox Manage a ManageEngine MDM.

Všechny důležité funkce na zařízeních byly otestovány a zařízení s nimi neměla problém. Hlavní rozdíl je ve vzhledu prostředí nebo aplikacích na zařízení, které komunikují s MDM serverem. Zprávy a notifikace na zařízeních se zobrazovaly přibližně ve stejném časovém intervalu, to stejné platí pro soubory a aplikace. Z pohledu administrátora po vyzkoušení jednoho softwaru, by neměl být problém přejít na jiný software, jelikož prakticky všechny funkce jsou stejné. Jediný problém pro administrátora bude se zorientovat v rozhraní.

Na závěr mohu sdělit, že většina softwarů pro správu mobilních zařízení nabízí totožné funkce a je tedy osobní preferencí zaměstnavatele nebo administrátora, které řešení zvolí. Nelze určit, který software je ten pravý, a který není pro správu zařízení ve firemním prostředí vhodný. Důležité je, aby si zaměstnavatel udělal rešerši svých mobilních zařízení ve firemním prostředí, následně udělal analýzu a zvolil správné MDM řešení.

Literatura

1. BANKMYCELL. *HOW MANY SMARTPHONES ARE IN THE WORLD?* 2021. Dostupné také z: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.
2. PIERER, Markus. *Mobile Device Management Mobility Evaluation in Small and Medium-Sized Enterprises*. Springer Fachmedien Wiesbaden, 2016. ISBN 9783658150457.
3. REED, Brian. *Test of 250 Popular Android Mobile Apps Reveals that 70% Leak Sensitive Personal Data*. 2019-06. Dostupné také z: https://www.nowsecure.com/blog/2019/06/06/test-of-250-popular-android-mobile-apps-reveal-that-70-leak-sensitive-personal-data/.
4. SAMSUNG. *Devices Secured by Knox*. 2021. Dostupné také z: https://www.samsungknox.com/en/knox-platform/supported-devices.
5. EVANS, Alma. *Mastering mobility management: MDM vs EMM vs UEM*. 2019-05. Dostupné také z: https://www.hexnode.com/blogs/mastering-mobility-management-mdm-vs-emm-vs-uem/.
6. DIGNAN, Larry. *Buying enterprise mobility management: How important is independence?* 2014-10. Dostupné také z: https://www.zdnet.com/article/buying-enterprise-mobility-management-how-important-is-independence/.
7. CAMERON, Randall. *MDM to EMM to UEM – a Mobile Journey*. 2018-04. Dostupné také z: https://www.mobile-mentor.com/insights/unified-endpoint-management-2018.
8. SILVA, Chris; BHAT, Manjunath; DOHENY, Rich; SMITH, Rob. *Magic Quadrant for Unified Endpoint Management Tools*. 2019-08. Dostupné také z: https://www.servasure.co/wp-content/uploads/2019/09/Gartner-Reprint-on-MobileIron.pdf.
9. SILVA, Chris; BHAT, Manjunath; DOHENY, Rich; SMITH, Rob; TAYLOR, Bryan. *Magic Quadrant for Unified Endpoint Management Tools*. 2018-07. Dostupné také z: https://b2bsalescafe.files.wordpress.com/2018/08/2018-gartner-magic-quadrant-for-unified-endpoint-management-tools-july-c3a9c3a08.pdf.
10. HEADWIND SOLUTIONS LTD. *Headwind MDM Version Comparison*. 2021. Dostupné také z: https://h-mdm.com/headwind-mdm-version-comparison/.

11. SAMSUNG. *Knox features on Android*. 2021. Dostupné také z: https://www.samsungknox.com/en/knox-features/android/manage.

12. MANAGEENGINE. *Edition Comparison Matrix*. 2021. Dostupné také z: https://www.manageengine.com/mobile-device-management-msp/edition-comparison-matrix.html?index.

13. ANDROID. *Overview*. 2020-10. Dostupné také z: https://developers.google.com/android/work/overview.

14. ANDROID. *EMMs Validated mobility management solutions that support Android Enterprise advanced and standard features*. Dostupné také z: https://androidenterprisepartners.withgoogle.com/emm.

15. ANDROID. *Devices*. 2021. Dostupné také z: https://androidenterprisepartners.withgoogle.com/devices/.

16. ANDROID. *Platform Architecture*. 2021. Dostupné také z: https://developer.android.com/guide/platform.

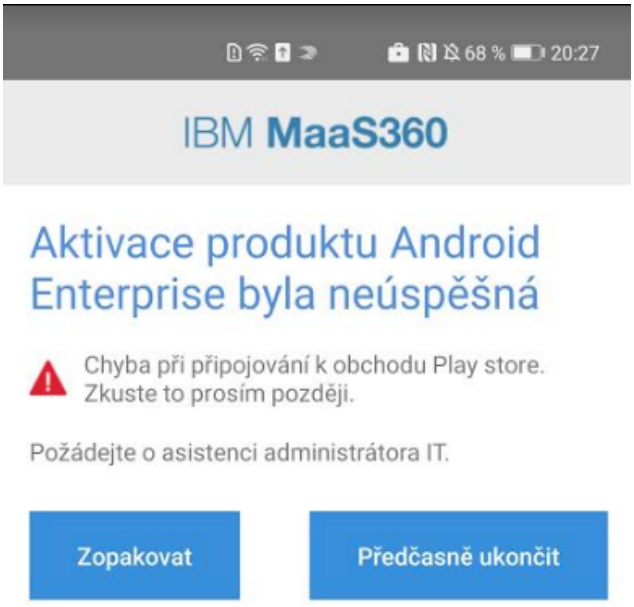
17. MOLÁČEKA, Petr; ČABOUN, Jan. *Jak vybrat vhodný systém pro mobile device management*. 2016. Dostupné také z: https://www.systemonline.cz/it-security/jak-vybrat-vhodny-system-pro-mdm.htm.

18. BAYTON, Jason. *Gartner comparison of security controls for mobile devices 2019*. 2020-02. Dostupné také z: https://bayton.org/download/doc/ae-general/Gartner_Comparison_of_Security_Controls_2019.pdf.

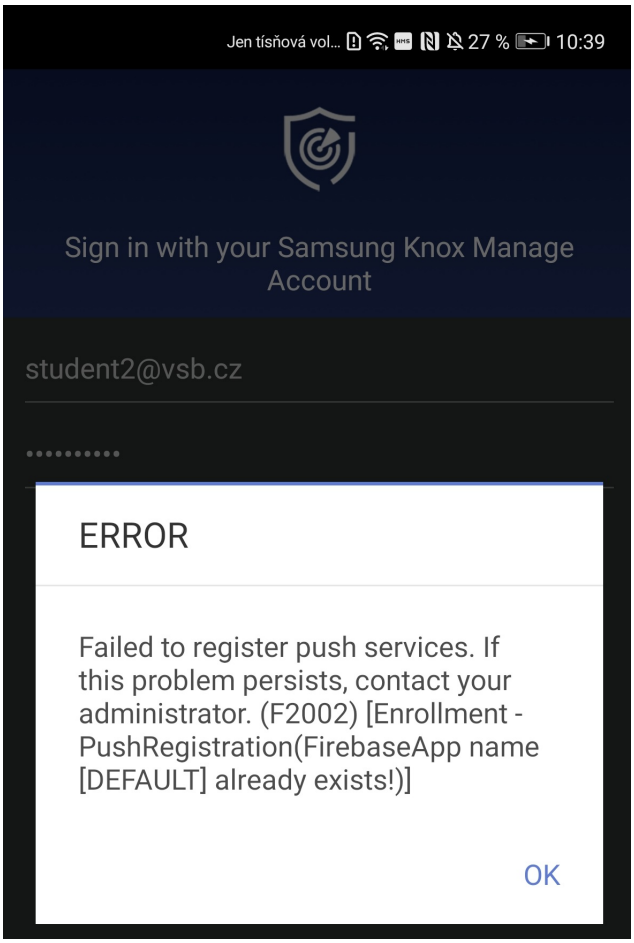
19. HEVESI, Patrick. *Mobile OSs and Device Security: A Comparison of Platforms*. 2019-05. Dostupné také z: https://www.gartner.com/en/documents/3913286.

Příloha A

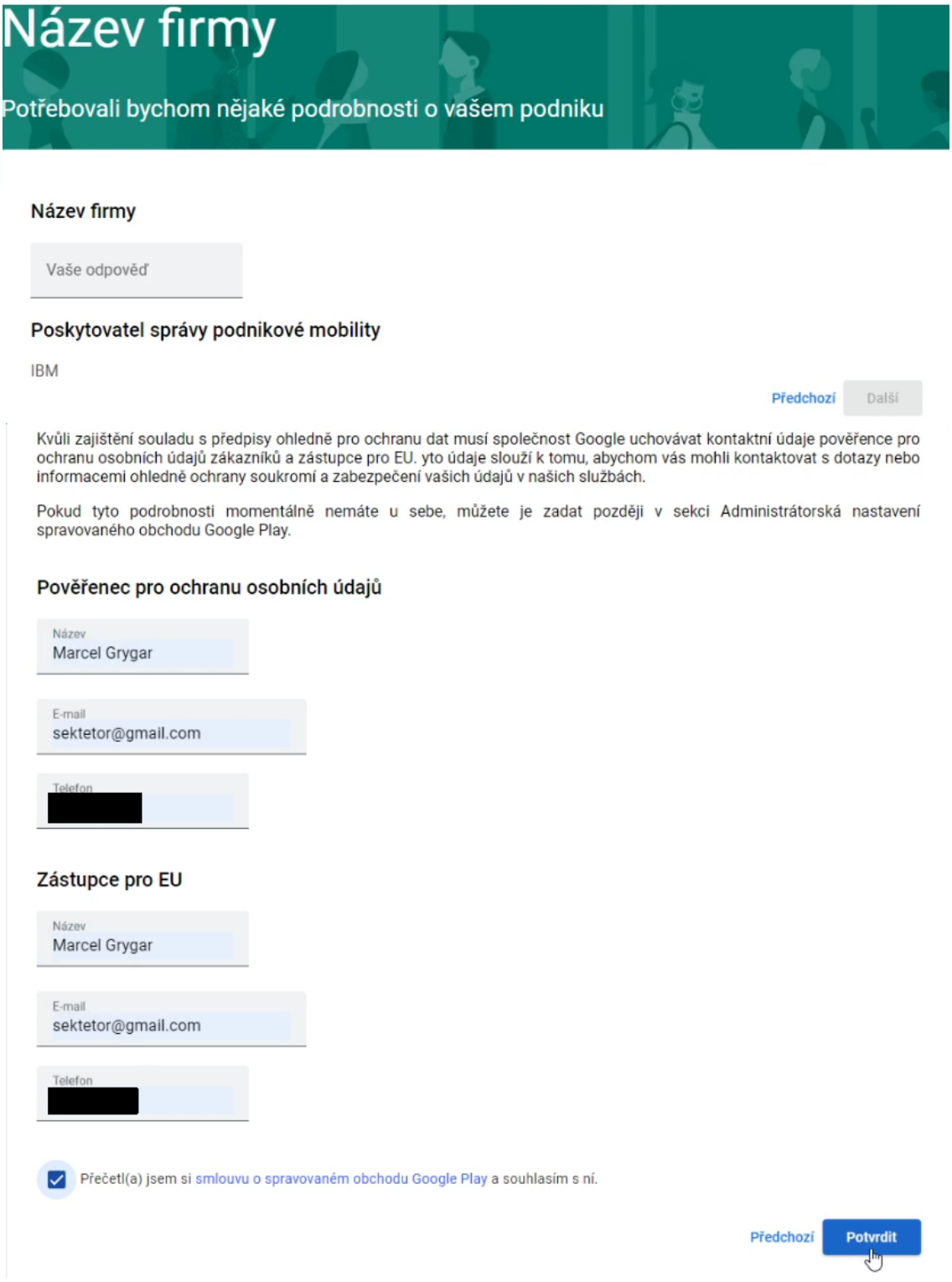
Obrázková příloha



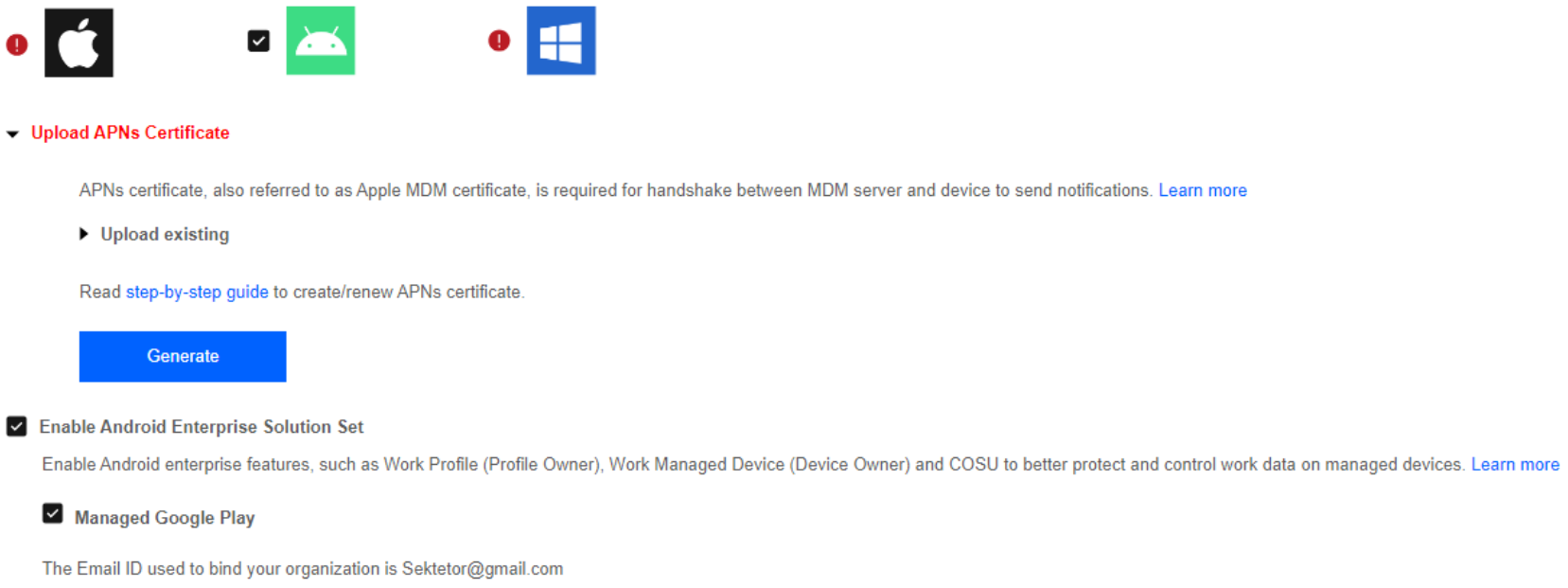
Obrázek A.1: Absence GMS na zařízení Huawei MaaS360



Obrázek A.2: Absence GMS na zařízení Huawei Knox Manage



Obrázek A.3: Registrace Google admistrátorského účtu



Obrázek A.4: Zprovoznění MaaS360 Mobile Device Managment